26.04.2022

Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ eelnõu seletuskiri

1. Sissejuhatus

Käesoleva eelnõuga kehtestatakse Vabariigi Valitsuse määrus „Võrgu- ja infosüsteemide küberturvalisuse nõuded“.

1.1. Sisukokkuvõte

Käesoleval eelnõul on kolm eesmärki.

1.1.1. Volitada küberturvalisuse eest vastutavat ministrit kehtestama Eesti infoturbestandardit (edaspidi *E-ITS*).

Eelnõu sätestab küberturvalisuse seaduse (edaspidi *KüTS*) § 7 lõike 5 volitusnormi alusel E-ITS-i kehtestamise volituse üleriigilise küberturvalisuse eest vastutavale ministrile, kelleks hetkel on ettevõtlus- ja infotehnoloogiaminister (edaspidi: minister).

E-ITS-i järgimise kohustust, sealhulgas auditeerimise kohustust kohaldatakse kogu KüTS kohaldamisalale, kuid nende täitmisel on ka erandid. E-ITS-i järgimise kohustus on asendatav ISO/IEC 27001:2017 (Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded)[1] järgimisega. Auditeerimise läbiviimine ei ole kohustuslik erasektoris mikroettevõtjale ning avalikus sektoris muuseumile, rahvaraamatukogule, etendusasutusele, valla või linna ametiasutuse hallatavale asutusele ja osavalla või linnaosa ametiasutuse hallatavale asutusele.

E-ITS asendab sisulises mõttes avaliku teabe seaduse (edaspidi *AvTS*) alusel kehtestatud infosüsteemide kolmeastmelist etalonturbe süsteemi (edaspidi *ISKE*). Sellest tulenevalt on määruse jõustumisel võimalik 2023. aastani (ISKE kehtetuks tunnistamiseni) jätkata ISKE täitmist E-ITS-i asemel ning on kehtestatud ka erinormid E-ITS-i rakendamiseks andmekogude suhtes.

1.1.2. Kehtestada avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded.

Eesmärgiks on tõsta Eesti omariikluse ja digitaalse järjepidevuse hoidmiseks loodud infotehnoloogiliste süsteemide aluseks oleva õigusruumi selgust ja läbipaistvust. Eelnõuga luuakse loetelu võrgu- ja infosüsteemidest (edaspidi *süsteem*), millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse asutuse võimele täita avalikke ülesandeid ning sätestatakse kohustus varundada nimetatud süsteemid välisriigis asuvasse turvalisse andmekeskusesse määruses ettenähtud tingimustel.

Olukorras, kus peaaegu kõik riigi avalikud teenused on digitaalselt kättesaadavad, on vajalik kindlustada riigi ja kohaliku omavalitsuse üksuse asutuste põhifunktsioonide täitmiseks vajalike andmete turvaline säilitamine ja ligipääs ning elutähtsate infosüsteemide töös hoidmine

[1] Standard leitav ning võimalik osta siit: https://www.evs.ee/et/evs-en-iso-iec-27001-2017.

teenuste osutamiseks ka siis, kui riigi territooriumil asuvate andmekeskuste töö on peatunud või häiritud näiteks sõja, looduskatastroofi, ulatusliku küberrünnaku, elektrikatkestuse või muu kriisiolukorra tõttu.

Hetkel varundatakse avalike ülesannete täitmist oluliselt mõjutavaid süsteeme ja nendes sisalduvaid andmeid Luksemburgi Suurhertsogiriigi riiklikku andmekeskusesse (edaspidi *Luksemburgi andmesaatkond*) Luksemburgi Suurhertsogiriigiga sõlmitud rahvusvahelise lepingu alusel[2]. Eelnõu valmimise hetkel on Luksemburgi andmesaatkonda varundatud juba e-toimiku süsteem, riigikassa infosüsteem, elektrooniline kinnistusraamat, maksukohustuslaste register, äriregister, riigi- ja kohaliku omavalitsuse asutuste riiklik register, mittetulundusühingute ja sihtasutuste register, kommertspandiregister, rahvastikuregister, elektrooniline kataster, sotsiaalkaitse infosüsteem, Riigi Teataja infosüsteem. Tulevikus on võimalus sõlmida rahvusvahelisi lepinguid andmete varundamiseks ka teiste välisriikidega lisaks Luksemburgi Suurhertsogiriigile.

1.1.3. Kehtestada pilvandmetöötlusteenusel põhineva süsteemi (edaspidi *pilvsüsteemi*) pidamise nõuded.

Eesmärk on võimaldada avalikul sektoril peetavaid süsteeme „pilve viia“ küberturvalisust tagaval viisil. Läbi pilvsüsteemi määratluse kehtestatakse nõuded, mida avalik sektor peab rakendama, kui soovib kasutada pilvandmetöötlusteenuseid. Raamistik on sellisel kujul küberturvalisuse tagamiseks vajalik, kuivõrd pilvandmetöötlusteenuse kasutaja tugineb suurel määral vastava süsteemi toimimiseks teenusepakkuja infrastruktuurile ning seadusandjal puudub jurisdiktsioonist tulenevatel põhjustel võimalus teenusepakkujatele avaliku sektori küberturvalisuse tagamiseks nõudeid kehtestada.

Nõudeid kohaldatakse KüTS § 3 lõikes 4 loetletud asutusele, kogule või isikule (koondnimetusega ning edaspidiselt *kasutaja*).

Peamised nõuded pilvsüsteemi pidamisel on järgnevad.

1) Teenusepakkuja usaldusväärsuse hindamise kohustus

Kasutaja peab enne pilvandmetöötlusteenuse hankimist hindama pakkuja usaldusväärasust ehk et kas teenusepakkujast tuleneb oht kasutaja süsteemide turvalisusele. Hinnatakse organisatsiooni ja tema taustast tulenevaid ohutegureid, mitte tehnilist lahendust.

2) Riikliku julgeoleku tagamisega seotud teabe teenusepakkujaga jagamise keeld

Kasutaja ei või spetsiifilist asutusesiseseks kasutamiseks tunnistatud teavet teenusepakkujaga pilvandmetöötluse kasutamise kontekstis jagada. Tegemist on kitsa ringiga kogu asutusesiseseks kasutamiseks tunnistatud teabest ning ei ole olulisel määral töödeldav avaliku sektori enamuse poolt. Nimetatud teabe majutamisel pilvsüsteemi peab teave olema teenusepakkuja vastu krüpteeritud (mis vähendab ka pilvandmetöötlusteenuse kasulikkust

[2] Eesti Vabariigi ja Luksemburgi Suurhertsogiriigi vaheline andmete ja infosüsteemide majutamise kokkulepe, RT II, 28.03.2018, 1; kättesaadav https://www.riigiteataja.ee/akt/228032018002.

sellise teabe töötlemise suhtes). Luuakse ministrile volitusnorm krüptomaterjalide täpsemate tehniliste nõuete kehtestamiseks.

3) Kasutaja organisatsiooniliseks toimepidevuseks olulistele pilvsüsteemidele alternatiivide pidamise kohustus.

Kui kasutaja soovib „pilve viia“ süsteemi, mis on kasutajale kui avaliku sektori organisatsioonile oluline oma ülesannete täitmiseks, siis peab kasutaja täiendavalt pidama ka alternatiivset süsteemi või meedet, mis võimaldab tal samu tegevusi teostada kasutatavast teenusest sõltumatult.

Vastava kohustusega süsteeme kaardistab kasutaja E-ITS-i rakendamise käigus. Alternatiivne süsteem või meede võib samuti olla pilvandmetöötlusteenus või isegi muu lahendus samalt teenusepakkujalt, kui see on tehnoloogiliselt iseseisev ehk üks töötab ilma teiseta. Alternatiivne meede peab suutma tagada samade ülesannete tegemise võimaluse, kuid ei pea olema pilvsüsteemiga tehniliselt samaväärne.

4) Pilvandmetöötlusteenuste kasutamisel kehtestatud tehniliste suvandite järgimine ja kasutamisega seonduvate logide edastamine Riigi Infosüsteemi Ametile (edaspidi *RIA*).

Sätestatakse ministrile volitusnorm levinumate pilvandmetöötlusteenuste kasutamisel rakendatavate tehniliste suvandite (kasutamise tehnilised seaded) kehtestamiseks. Volitusnormi alusel kehtestatud juhendi olemasolul rakendab kasutaja sätestatud tehnilisi suvandeid.

Sätestatakse kohustus edastada või tagada muul moel juurdepääsu RIA-le pilvandmetöötlusteenuse kasutamisega seonduvatele logidele, mis võimaldavad analüüsida pilvsüsteemi turvalisust. Logid tuleb edastada RIA-le reaalajas. Kui teenusepakkuja kasutajale vastavate logidele ligipääsu ei võimalda, puudub ka kohustus nende edastamiseks. Erandiks on olukorrad, kus pilvsüsteem töötleb julgeolekuga seotud teavet või on organisatsiooni toimepidevuseks oluline. Sellisel juhul kasutatakse vaid neid teenusepakkujaid, mis logisid ka kasutaja edastavad.

1.2. Eelnõu ettevalmistajad

Määruse eelnõu ja seletuskirja koostasid Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunikud Oliver Grauberg (oliver.grauberg@mkm.ee) ja Raavo Palu (raavo.palu@mkm.ee) ning digiriigi arengu osakonna IT-õiguse nõunik Kätlin Aren (katlin.aren@mkm.ee).

Eelnõu ja seletuskirja osas tegi õiguslikke ettepanekuid Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna õigusnõunik Ave Henberg (ave.henberg@mkm.ee). Eelnõu ja seletuskirja toimetas keeleliselt Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@mkm.ee).

1.3. Märkused

Eelnõu on seotud küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse eelnõuga 531 SE (edaspidi *531 SE*), millega luuakse volitusnorm käesoleva määruse kehtestamiseks.[3]

Määrus kehtestatakse küberturvalisuse seaduse § 7 lõike 5 alusel.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb neljast peatükist. Esimene peatükk reguleerib määruse üldsätteid, teine peatükk sisustab E-ITS-iga seotud sätteid, kolmas peatükk sisustab turvameetmete nõuded (eraldi jagudena nii turvameetmete üldnõuded kui ka erinõuded, sh jaguneb teine jagu kolmeks jaotiseks: andmekogud, avalike ülesannete täitmist oluliselt mõjutatavad süsteemid ja pilvesüsteem) ning neljas peatükk sisustab rakendussätted.

Eelnõu § 1 kehtestab eelnõu reguleerimisala. Määruse reguleerimisala vastab KüTS § 7 lõike 5 alusel kehtestatud volitusnormi sisulisele piiritlusele.

KüTS § 7 lõikes 5 sätestatud edasivolituse alusel sätestab eelnõu volituse küberturvalisuse tagamise korraldamise eest vastutavale ministrile E-ITS-i kehtestamiseks.

Täiendavalt sätestab eelnõu volituse küberturvalisuse tagamise korraldamise eest vastutavale ministrile süsteemide erinõuete kehtestamiseks. Volitus sätestatakse kahte liiki erinõuete kehtestamiseks. Esiteks sätestatakse volitus pilvsüsteemi pidamiseks kasutatava pilvandmetöötlusteenuse kohustuslike tehniliste suvandite kehtestamiseks, mis on selgitatud eelnõu § 15 lõike 2 alajaotises. Teiseks sätestatakse volitus pilvsüsteemis eelnõus piiritletud teabe krüpteerimise krüptomaterjalide nõuete kehtestamiseks, mis on selgitatud eelnõu § 17 lõike 3 alajaotises.

Eelnõu § 2 kehtestab määruses kasutatavate terminite tähenduse, sisustatakse andmekogu, inforturve ja pilvsüsteemi terminid. Eelnõus avamata terminid on KüTS tähenduses, sealhulgas teenuse osutaja.

Andmekogu on andmekogu avaliku teabe seaduse § 43^1 lõike 1 tähenduses.

Esimese uue terminina kasutatakse mõistet „infoturve“. Infoturbena käsitletakse terviklikku protsessi, mille lõppeesmärk on turvameetmete rakendamine, mistõttu hõlmab termin ka turvameetmete loomise ja valimise protsesse.

Teise uue terminina kasutatakse mõistet pilvsüsteem ehk pilvandmetöötlusteenusel põhinev süsteem. Selle termini selgitamiseks on vaja käsitleda termini kolme peamist komponenti –

[3] Küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seadus 531 SE – kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/K%C3%BCberturvalisuse%20seaduse,%20avaliku%20teabe%20seaduse%20ja%20Eesti%20Rahvusringh%C3%A4%C3%A4lingu%20seaduse%20muutmise%20seadus.

pilvandmetöötlusteenus, süsteem ning pidamine (ehk süsteemi pidamine pilvandmetöötlusteenust kasutades).

Pilvandmetöötlusteenus on KüTS-s defineeritud termin. Tegemist on infoühiskonna teenusega, mis võimaldab juurdepääsu andmetöötlusressursside kogumile, mis on paindlikult jagatav ning laiendatav süsteemi ennast muutmata. KüTS-i termin on üle võetud NIS direktiivist.[4] Termin käsitleb väga laia valdkonda, kuivõrd kõik infoühiskonna teenused,[5] mis nimetatud kriteeriumitele vastavad, on käsitletavad pilvandmetöötlusteenusena. Näiteks lisaks lihtsamatele serverite „rentimisele" kohaldub see termin ka tarkvaralistele lahendustele, mille funktsioonid tuginevad teenusepakkuja andmetöötlusressurssidele ning mis pakuvad kitsamaid andmetöötlusfunktsioone, sest NIS direktiivi selgituspunktis 17 on mõiste „laiendatav" (direktiivi tõlkes mõiste „skaleeritav") kirjeldatud just teenusepakkuja võimekusena vastavalt vajadusele ressursse ühe kasutaja jaoks laiendada. Samuti on Euroopa Komisjon täpsustanud[6] et pilvandmetöötlusteenusena on käsitletav ka tarkvarana pakutud teenus (*software as a service* ehk *SaaS*). Teisisõnu võib pilvandmetöötlusteenustena olla käsitletav ka tüüpiline kontoritarkvara, kui pakutav teenus vastab toodud kriteeriumitele. On ka oluline märkida, et termini alla ei kohaldata tegevusi, mis on küll sisult sarnased, kuid ei ole infoühiskonna teenused (näiteks ei ole osutatud majandus- või kutsetegevuse raames).

Süsteem on samuti KüTS-s defineeritud termin. Tegemist on laia mõistega, mis ei piirdu ainult tehnoloogilise riistavaraga, vaid laieneb ka tarkvarale ning digitaalsetele andmetele. KüTS-i subjekti süsteem käesoleva pilvsüsteemi mõiste kontekstis ei ole seega üldjuhul riistvara, sest pilvandmetöötluse peamine eeldus on, et andmetöötlusressursid on teenusepakkuja valduses, mitte kasutaja valduses. Pilvsüsteemi kontekstis käsitletakse seega süsteemina ennekõike kasutaja kasutatavat tarkvara ning andmeid, mis vastavatel ressurssidel majutatud on või nende toel funktsioneerivad. On oluline eristada, et lihtsalt pilvandmetöötlusteenuse kasutamine ei tähenda, et subjektil puudub kaardistatav ning kaitstav infovara pilvandmetöötlusteenusel tuginevate protsesside küberturvalisuse tagamisel.

Pilvsüsteem on seega süsteem (ennekõike tarkvaralisel ja andmete kujul), mida peetakse pilvandmetöötlusteenuse kaudu ehk pakutud andmetöötlusressursse kasutades. Pilvsüsteem võib seega olla nii pilves majutatav andmekogu kui ka KüTS-i subjekti teabevahetuse protsessi infovarad.

---

[4] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.07.2016, lk 1-30) – kättesaadav: https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX:32016L1148.

[5] Infoühiskonnateenuse seaduse § 2 punkt 1: infoühiskonna teenus – teenus, mida osutatakse majandus- või kutsetegevuse raames teenuse kasutaja otsesel taotlusel ja mille puhul andmeid töödeldakse, säilitatakse ja edastatakse digitaalkujul andmete töötlemiseks ja säilitamiseks mõeldud elektrooniliste vahendite abil, kusjuures osapooled ei viibi üheaegselt samas kohas. Infoühiskonna teenus peab olema täielikult üle kantud, edastatud ja vastu võetud elektrooniliste sidevahendite abil. Infoühiskonna teenus ei ole faksi ega telefonikõne abil edastatud teenus ega televisiooni- või raadioteenus.

[6] Komisjoni teatis Euroopa Parlamendi ja nõukogule: Parimate tulemuste saavutamine võrgu- ja infoturbe direktiivi rakendamisel – jõupingutused direktiivi (EL) 2016/1148 (meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus) tulemuslikuks rakendamiseks (COM/2017/0476 final, 13.09.2017 ning uuendatud 04.10.2017) – kättesaadav: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476.

Eriliigiliste süsteemide turvameetmete nõuete kehtestamisel määruse 3. peatükis sätestatakse ka erisusi E-ITS-i nõuete järgimise osas, millest tulenevalt kasutatakse määruses ka kehtestatava E-ITS-i termineid vastavalt E-ITS-is sätestatud tähendustele.

Eelnõu § 3 sätestab E-ITS-i kehtestamise volituse ning E-ITS-i rakendamise erandi.

Lõige 1 kehtestab volitusnormi E-ITS-i kehtestamiseks. E-ITS, kui käesoleva eelnõu koostamise hetkel ligikaudu 500-leheküljeline kogum nõuetest ja juhenditest, kehtestatakse küberturvalisuse tagamise korraldamise eest vastutava ministri määrusega.

Sarnaselt hetkel kehtiva ISKE-ga on ka E-ITS pidevat kaasajastamist ning täiendamist nõudev dokument. Majandus- ja Kommunikatsiooniministeeriumi (edaspidi *MKM*) valitsemisala asutus RIA korraldab E-ITS-i täiendamise ning uuendamisega seotud teenuseid, võttes selle aluseks varasemase rakendamise praktikat ning muutusi infotehnoloogilises maailmapildis ja õigusraamistikes. Tulenevalt eeldatavast vajadusest E-ITS-i korduvalt muuta ja ajakohastada ei ole Vabariigi Valitsuse määruse vorm sobilik E-ITS-i kehtestamiseks. Sellegipoolest omab E-ITS-i kehtestamine regulatiivset mõju ning ei ole käsitletav üksikjuhtumi reguleerimisena oma rakendusala tõttu, mistõttu on välistatud E-ITS-i kehtestamine käskkirjaga. Eesmärgipärane vorm E-ITS-i kehtestamiseks ongi eeltoodust lähtuvalt ministri määrus.

Eelnõuga kehtestatava määruse volitusnorm (KüTS § 7 lõige 5) hõlmab ka edasivolituse võimalust haldusmenetluse seaduse § 91 lõike 1 tähenduses. E-ITS-i dokumentatsioon ning muu E-ITS-ga seotud teave avalikustatakse ka Eesti infoturbestandardi portaalis - eelnõu koostamise hetkel asub see veebiaadressil https://eits.ria.ee/.

Kehtestatav ministri määrus kehtestab E-ITS-i dokumentatsiooni ja sisustab E-ITS-i rakendamise kohustust.

Lõige 2 määratleb, et süsteemi turvalisuse tagamiseks rakendatud meetmete vastavust E-ITS-le eeldatakse ka juhul, kui selle asemel rakendatakse rahvusvahelist standardit ISO/IEC 27001:2017 (Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded).[7]

E-ITS-i võimalik alternatiiv on rahvusvahelise standardi ISO/IEC 27001 järgimine. Samas ei piisa selle alternatiivi kasutamiseks lihtsalt teenuse osutaja otsusest ega ka standardi rakendamisele vastavatest tegevustest. Alternatiiv kuulub kohaldamisele vaid siis, kui teenuse osutaja on lisaks ISO/IEC 27001 standardi nõuetele vastavate turvameetmete rakendamisele esitanud RIA-le kehtiva ISO/IEC 27001 vastavussertifikaadi, mille kohaldamisala hõlmab vähemalt E-ITS-i kohaldamisala. Kui teenuse osutaja RIA-le eelnevalt kehtivat vastavussertifikaati esitanud ei ole, on teenuse osutaja vastavus eelnõu E-ITS-le hinnatav sõltumata sellest, kas teenuse osutaja on vastavuses ISO/IEC 27001 nõuetega, isegi kehtiva vastavussertifikaadi olemasolul. Selle kitsenduse eesmärk on tagada järelevalveasutusele ülevaade teenuse osutajate vastavusest E-ITS-i järgimise nõuetele ning kuivõrd E-ITS-i vastavusauditite järeldusotsuste edastamine RIA-le on kohustuslik, siis alternatiivi rakendamine ilma aktiivse edastamiskohustuseta töötaks ülevaate tagamise eesmärgi vastu.

[7] Standard leitav ning võimalik osta siit: https://www.evs.ee/et/evs-en-iso-iec-27001-2017.

Erinevalt eelnõu §-s 20 toodud võimalustest (vt sealsete lõigete selgitust) pole siinse lõikega tekitatav erand ajutine.

Eelnõu § 4 kehtestab E-ITS-i tingimuste täitmise auditeerimise nõuded.

E-ITSi tingimuste täitmise üks osa on auditeerimine ning seda aitab sisustada E-ITS-i osaks olev auditeerimisjuhend. Auditeerimise nõudeid ei kohaldata teenuse osutajale, kes on täitnud eelnõu § 3 lõike 2 tingimused, kuivõrd nende osas loetakse auditeerimiskohustus, kui E-ITS-i järgimiskohustuse üks osa, täidetuks viidatud sätte tõttu.

Lõige 1 kehtestab auditeerimise põhilise nõude – audit viiakse läbi iga kolme aasta järel. Esmakordse auditi läbiviimise tähtaeg on üldjuhul 3 aastat alates auditeerimise kohustuse tekkimisest. Teenuse osutajatele, kellele tekib auditeerimise kohustus eelnõu jõustumise hetkel, sh kes on eelnevalt turvameetmete süsteemi rakendamise auditeerimist läbi viinud ISKE nõuete järgi, sätestavad esmakordse auditi läbiviimise tähtaja eelnõu 4. peatüki rakendussätted.

Teenuse osutajate loetelu on sätestatud KüTS § 3 lõikes 1. Lisaks selles lõikes nimetatud isikutele kohaldatakse teenuse osutaja kohta sätestatud nõuded ka KüTS § 3 lõikes 4 sätestatud loetelus olevatele isikutele (vt siin ka 531 SE-ga tehtavaid muudatusi).

Selleks, et läbiviidav audit oleks aluseks auditeerimise kohustuse täitmisele, peab auditi planeerimine, tegemine jm tegevused (ehk auditeerimine) toimuma vastavalt eelnõu § 3 lõike 1 alusel kehtestatud auditeerimisjuhendile.

Audit loetakse käesoleva lõike tähenduses läbiviiduks, kui audiitor on teenuse osutajale edastanud auditeerimisjuhendi tähenduses lõpparuande. Sellest hetkest alustab kulgemist järgmise auditi läbiviimise tähtaeg ning teenuse osutaja kohustus on tagada vastavaks tähtajaks järgmise auditi läbiviimine. Kuna infoturbe haldus on kestev protsess, siis praktikas tuleb teenuse osutajal hakata tegelema lõpparuandes toodud puuduste likvideerimisega (kui neid tuvastatakse) selleks, et saavutada positiivne tulemus järgmisel auditil.

Ei ole keelatud auditi läbiviimist, ennekõike auditi tellimist, volitada või teha koos teise organisatsiooniga. Ühisauditite läbiviimine või teise organisatsiooni nimel auditi tellimine on ennekõike asjakohane olukordades, kus erinevate organisatsioonide info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) infrastruktuuri haldamine ja majutamine on üle antud kesksele organisatsioonile. Küll aga peab läbiviidud auditi lõpparuanne käsitlema teavet iga auditi subjekti suhtes. IKT infrastruktuuri haldamine ja majutamine kolmanda organisatsiooni kaudu ei mõjuta auditi subjekti iseseisvat kohustust E-ITS-i järgida, mille täitmist auditeerimine kontrollib.

Lõige 2 kehtestab kohustuse lõike 1 alusel läbiviidud auditi järeldusotsuse edastamiseks järelevalveasutusele. Kohustus on eraldiseisev auditeerimise (ja seetõttu ka E-ITS-i järgimise) kohustusest. Teisisõnu ei loeta käesolevas lõikes kehtestatud kohustuse täitmisel teenuse osutaja poolt täidetuks auditeerimise kohustust ega ka muid eelnõu § 3 lõike 1 alusel kehtestatud kohustusi. Samamoodi on läbiviidud auditi järeldusotsuse esitamata jätmisel teenuse osutaja rikkunud käesoleva lõike alusel kehtestatud kohustust sõltumata sellest, kas teenuse osutaja on täitnud E-ITS-i järgimise, sh auditeerimise kohustust.

Lõike kohaselt täidab kohustuse teenuse osutaja, kuid praktikas on ka võimalik, et teenuse osutaja on selle ülesande edasi delegeerinud talle auditi tellinud IT-majale (avaliku sektori korral) või muule välisele partnerile (kui taoline olukord ilmneb).

Lõike 3 eesmärk on tagada E-ITS-i nõuete järgimisest tulenevate kohustuste proportsionaalsus subjekti IKT korralduslike võimetega.

Subjektidele, kes vastavad käesolevas lõikes kehtestatud tingimustele, on auditi läbiviimine valikuline ja soovitatav, kuid mitte kohustuslik osa E-ITS-i järgimise kohustusest. See aga ei tähenda, et E-ITS-i järgimine tervikuna oleks subjektile valikuline või et E-ITS-i järgimine ei oleks subjekti suhtes järelevalvatav. Auditi läbiviimise valikulisus ei mõjuta KüTS-is määratletud järelevalveorgani meetmete rakendamist subjektide suhtes nõuete täitmise tagamiseks ega sätesta ühtki eeldust, et subjekt E-ITS-i järgimisest tulenevaid nõudeid muus osas täidab. Sellest tulenevalt on ka auditi läbiviimine soovitatav sõltumata selle tegemise kohustusest.

Esimene erand on sätestatud lõike **esimeses punktis**. Sellest tulenevalt on audit valikuline KüTS-i subjektidele, kes vastavad mikroettevõtja definitsioonile. Tegemist on väikesemahuliste organisatsioonidega, kelle IKT korralduslikud vahendid on oluliselt piiratumad ning seetõttu võib ka auditi lävendiline majanduslik mõju olla organisatsioonile ebaproportsionaalselt suur. KüTS-i subjektidest on mikroettevõtjad enamasti teede sõidetavust tagavad ettevõtjad (subjektid KüTS § 3 lg 1 p 1 alusel hädaolukorra seadusest tulenevalt) ning mitmed perearstid (subjektid KüTS § 3 lg 1 p 7 alusel).

Teine erand on sätestatud lõike **teises punktis**. Tegemist on asutustega, mille IKT korralduslikud vahendid on oluliselt piiratumad tulenevalt IKT vahendite väiksemast olulisusest asutuse avalike ülesannete täitmisel. Avalikus sektoris sõltub asutuse IKT struktuuri mahukus ning selle IKT struktuuri turvalisuse kriitilisus ühiskonna toimepidevusele rohkem asutuse ülesannetest kui asutuse organisatsioonilisest suurusest. Muuseumi all on mõeldud muusemi muuseumiseaduse § 2 lõike 1 tähenduses ning hõlmab sama seaduse § 1 lõigetes 2 ja 3 nimetatud muuseumeid.[8] Rahvaraamatukogu all on mõeldud rahvaraamatukogu seaduse § 2 lõike 2 tähenduses olevat rahvaraamatukogu.[9] Omavalitsusüksuse ametiasutuse hallatava asutuse all on mõeldud asutusi, mis on asutatud kohaliku omavalitsuse korralduse seaduse § 22 lg 1 punkti 34 alusel.[10]

Kommenteeritavas punktis nimetatud asutused peavad siiski läbima auditi, kui vastav asutus on haridusasutus (Eesti Vabariigi haridusseaduse[11] § 3 lõikes 2 tähenduses) või kui tegemist on andmekogu vastutav töötleja või volitatud töötleja (AvTS § 43^4 tähenduses). Neid asutusi ei välistata auditi tegemise ja auditi järeldusotsuse edastamise kohustustest nende asutuste täidetavate ülesannete tõttu.

[8] Muuseumiseadus, RT I, 19.03.2019, 103.
[9] Rahvaraamatukogu seadus, RT I, 13.03.2019, 127.
[10] Kohaliku omavalitsuse korralduse seadus, RT I, 25.06.2021, 8.
[11] Eesti Vabariigi haridusseadus, RT I, 16.06.2020, 3.

Eelnõu §-id 5 ja 6 kehtestavad turvameetmete üldnõuded 3. peatüki eraldi jaona. **Eelnõu § 5** kehtestab teenuse osutaja teenuste kaardistuse ja turvameetmete dokumenteerimiskohustuse.

Lõige 1 täpsustab dokumenteerimisnõudeid. KüTS § 7 lg 2 punkti 1 alusel peab teenuse osutaja koostama süsteemi riskianalüüsi, mis lähtub küberintsidentide ohust ning ohu realiseerumisel kahju olulisusest. Riskianalüüs kuulub ise dokumenteerimisele KüTS § 7 lg 2 punkti 2 alusel, samuti ka turvameetmete kirjeldus. Kuid küberriskide haldamisel on mainitud kohustuse näol tegemist vaid kahe viimase protsessi dokumenteerimisega.

Riskianalüüsi läbiviimisele eelneb teenuste kaardistamine ning nende teenuste haldamiseks asjakohaste süsteemide kaardistamine. Käesolev lõige sätestab seega ka kohustuse dokumenteerida lisaks riskianalüüsile ja rakendatavatele turvameetmetele ka riskianalüüsile eelnev teenuste ja vastavate süsteemide kaardistus. Teenuste kaardistamine erasektori puhul on seotud KüTS § 3 lõikes 1 vastava punkti juures viidatud osutatava teenusega. Avaliku sektori puhul siinses lõikes mõeldud kaardistus ei ole täielikult kattuv kaardistusega, mis valitsusasutused peavad tegema teenuste korraldamise ja teabehalduse aluste määruse (edaspidi *TKTA määrus*)[12] § 7 lõike 1 alusel, kuna TKTA määrus kehtib ainult valitsusasutustele, kuid KüTS-i ning siinse eelnõuga kehtestatava määruse nõuded kehtivad ka muudele isikutele ja asutustele kui valitsusasutused. Siiski on võimalik siinse kaardistuse puhul arvestada ning kasutada TKTA määruse täitmiseks tehtud kaardistust või teha koos tolle kaardistusega (vt ka eelnõu § 5 lõike 3 selgitust).

Lõige 2 täpsustab riskianalüüsi ja sellega seonduva dokumentatsiooni säilitamisnõuded. KüTS § 7 lg 2 punkti 2 alusel on teenuse osutaja kohustatud tagama riskianalüüsi ja sellega seonduva dokumentatsiooni olemasolu. Käesolev lõige sisustab eelmainitud kohustuse vähemalt 7 aastase säilitamiskohustusega.

KüTS § lg 2 punkti 6 kohaselt peab teenuse osutaja juba praegu taolist dokumentatsiooni säilitama vähemalt kolm aastat dokumendi loomisest alates. Vastav KüTS-i nõue tunnistatakse 531 SE-ga kehtetuks ning selle asemel kehtestatakse samalaadne (pikema tähtajaga) säte siinse eelnõuga. Kui teenuse osutaja on koostanud nimetatud KüTS-i nõude alusel vastava dokumentatsiooni ning see on säilitatud alla kolme aasta eelnõu jõustumise kuupäeval, siis edaspidiselt tuleb nimetatud dokumentatsiooni säilitada vähemalt 7 aastat. Tähtaja määratlemisel on lähtutud asjaolust, et see tähtaeg katab ära vähemalt kaks auditiperioodi (3+3 aastat) ning ühe aastase täiendava tähtaja. Nimetatud tähtaeg võimaldab järelevalveasutusel ka planeerida enda järelevalvelisi tegevusi.

Täiendavalt sätestab käesolev lõige kohustuse lõikes 1 nimetatud dokumentatsiooni järelevalveasutusele kättesaadavaks tegemiseks. Sätte eesmärk on küberturvalisuse nõuete järgimise järelevalve efektiivsemaks muutmine. Riskianalüüs ja sellega seonduv on suuresti aluseks teenuse osutaja küberturbe võimekuse ning selle valdkonna nõuete täitmise hindamisele. RIA kui järelevalveasutus saab käesolevale sättele tuginedes nõuda teenuse osutajalt lõikes 1 nimetatud dokumentatsiooni.

[12] Vabariigi Valitsuse 25.04.2017 määrus nr 88 „Teenuste korraldamise ja teabehalduse alused“, RT I, 25.03.2021, 6.

Lõige 3 täpsustab koostatava dokumentatsiooni vormilisi võimalusi. Käesolev lõige sätestab, et lõikes 1 nimetatud dokumentatsioon võib olla samastatav teenuse osutaja poolt muu õigusakti alusel koostatava dokumendi osana. Üheks näiteks on E-ITSi järgimise kohustuse täitmiseks koostatav dokumentatsioon. Teiseks näiteks on TKTA määruse alusel tehtavad kaardistused (vt TKTA määruse § 7 lõiget 1 ja § 12 lõiget 1).

Muu õigusakti alusel koostatava dokumendi osa vastavus lõikes 1 nimetatud dokumentatsiooni nõuetele sõltub võrreldavate sisulisest analüüsist. Selleks, et muu õigusakti alusel koostatava dokumendi osa oleks samastatav lõikes 1 nimetatud dokumentatsiooniga, peab vastav dokumendi osa sisaldama lõikes 1 nimetatud dokumentatsiooni sisu, st peab olema olemas teenuste ja nende haldamiseks asjakohaste süsteemide kaardistus, riskianalüüs ja süsteemidele rakendatavad turvameetmed.

Vorminõude täpsustus rakendub KüTS § 7 lg 2 punktides 1 ja 2 nimetatud dokumentidele, kuivõrd täpsustavad dokumenteerimisnõuded on nende osas kehtestanud kommenteeritava paragrahvi lõige 1.

Käesoleva lõike vormilise võimaluse kasutamisel lõikes 1 nimetatud dokumenteerimiskohustuse täitmisel kohustub teenuse osutaja RIA lõikele 2 tugineva taotluse alusel esitama kas muu õigusakti alusel koostatud dokumendi tervikuna või vähemalt sellises osas, et esitatavas dokumentatsioonis kajastuks lõikes 1 nõutud sisu.

Eelnõu § 6 täpsustab, millal tuleb eelnevas paragrahvis mainitud riskianalüüs ajakohastada.

KüTS § 7 lg 2 punkti 2 alusel on teenuse osutaja kohustatud tagama riskianalüüsi ajakohasuse. Käesolev lõige sisustab eelmainitud kohustuse. Riskianalüüsi ajakohastamise tähtpäev on kõige hiljemalt kolme aasta möödumisel viimasest riskianalüüsi ajakohastamisest. Kahel alternatiivsel juhul võib aga riskianalüüsi ajakohastamise tähtpäev saabuda varem.

Esiteks peab teenuse osutaja oma koostatud riskianalüüsi ajakohastama viivitamatult pärast olulise mõjuga küberintsidendi toimumist. Pärast olulise mõjuga küberintsidendi toimumist on vajalik edasiste intsidentide ennetamiseks vaadata üle ennekõike riskianalüüsis loetletud riskide ning nendele määratud tagajärgede raskusastmete asjakohasus. Küberintsident on defineeritud KüTS § 2 punktis 3 ning küberintsident on olulise mõjuga, kui on täidetud vähemalt üks KüTS § 8 lõikes 2 sätestatud tingimustest.

Teiseks peab teenuse osutaja oma koostatud riskianalüüsi ajakohastama viivitamatult pärast süsteemi turvalisust mõjutava muudatuse rakendamist. Sellises olukorras ei pruugi enam olla asjakohased riskianalüüsi aluseks olevate süsteemide kaardistused ega ka riskianalüüsis loetletud riskid ning nende tagajärgede raskusastmed. Süsteemi turvalisus on defineeritud KüTS § 2 punktis 2 ning süsteemi turvalisust mõjutava muutusena on käsitletavad kõik muudatused süsteemile (nii riist– kui ka tarkvaralised) mis mõjutavad süsteemi eelmainitud omadust. Riskianalüüsi ajakohastamise kohustuse tekkimiseks peab muudatus olema läbiviidud või tellitud teenuse osutaja poolt. Litsentseeritud tarkvara suhtes rakendatavad uuendused litsenseerijate poolt, kui need on tehtud süsteemi tavapärase hoolduse raames ning ei muuda süsteemi otstarvet, ei too kaasa ka kohustust riskianalüüsi ajakohastamiseks.

Tuvastamine, kas teenuse osutaja on viivitanud riskianalüüsi ajakohastamisega, tuleb läbi viia iga teenuse osutaja suhtes asjaoludest lähtuvalt. Ennekõike on viivitamise tuvastamisel oluline riskianalüüsi ajakohastamise eeldatav ajakulu muudatuste ning mõjutatud süsteemide ulatust arvestades. Pärast küberintsidendi toimumist tuleb viivituse tuvastamisel arvestada ka võimaliku ajakuluga KüTS § 7 lg 2 punktis 4 sätestatud kohustuse täitmiseks.

Eelnõu §-id 7 kuni 11 (3. peatüki 2. jao 1. jaotis) kehtestavad küberturvalisuse nõuete erisused andmekogude pidamisel. Andmekogu on AvTS-s reguleeritud süsteemi eriliik, millele rakenduvad ka eelmainitud seaduse alusel mitmed nõuded. Andmekogude küberturvalisuse tagamiseks rakendatakse ISKE nõudeid, mis omakorda olid koostatud andmekogu kui süsteemi vaatepunktist. E-ITSi kehtestamisel ISKE asemele (531 SE ning siinse eelnõu tulemusena) uueneb mõnevõrra ka küberturvalisuse tagamiseks rakendatavate nõuete loogika, seda ennekõike süsteemipõhise lähenemise asendamisel organisatsiooni ja selle protsesside põhiste lähenemisega.

Arvestades aga vajadust säilitada andmekogude kui eriliigiliste süsteemide turbeastme määramine ennekõike andmekogu andmete tähtsusest lähtuvalt (erinevalt E-ITS-i riskipõhisest kaitsetarviduse määramisest infovarade olulisuse kaudu protsessi eesmärgi täitmisel) ning säilitada riigi infosüsteemi haldussüsteemi ja seekaudu ka andmekogude põhimääruste regulatiivne sisu turvaosaklasside ja nendest tulenevate turbetasemete osas, on eelnõu §-de 7-11 eesmärk võtta üle kehtetuks tunnistatavast[13] infosüsteemide turvameetmete süsteemist andmekogude turbeastmete regulatsioon ning ühildada see E-ITS-i rakendamisega organisatsioonis, mis on andmekogu vastutav või andmekogu majutav volitatud töötleja.

Eelnõus sätestatavad §-id 7-10 kehtivad juba praegu süsteemidele (vt KüTS § 9 lõiget 2), sh andmekogudele (vt AvTS § 43[9] lõike 3 esimest lauset ning sama paragrahvi lõike 1 punkti 4). Need nõuded on hetkel sisustatud Vabariigi Valitsuse 20.12.2007 määruse nr 252 „Infosüsteemide turvameetmete süsteem“ (edaspidi *ISKE määrus*)[14] §-des 4-9. Nimetatud muudatusete sisu on analüüsitud ISKE määruse ning selle muudatuste vastu võtmisel – seetõttu puudub vajadus kehtiva õiguse säilitamisega seotud muudatusi uuesti analüüsida.

Eelnõu §-id 7–11 hakkavad kehtima 01.01.2023 ehk ISKE määruse volitusnormi kehtetuks tunnistamise järel.

Eelnõu § 7 kehtestab turvameetmete nõuete erisused andmekogu pidamisel.

Lõige 1 kehtestab andmekogu vastutavale töötlejale kohustuse korraldada andmekogu turbeastme määramine. Andmekogu turbeastme määramise aluseks on andmekogu andmete turvaklass, mille määramist samuti andmekogu vastutav töötleja korraldama peab. Andmekogu andmete turvaklassi määramise aluseks on andmete turvaanalüüs ehk andmete tähtsuse hindamine ning andmete püüdmisest tuleneva kahju hindamine, ka selle läbiviimise kohustus on andmekogu vastutaval töötlejal käesoleva lõike alusel. Eelnõu § 10 sisustab täpsemalt andmete turvaanalüüsile vastavate erinevate andmete turvaosaklasside olemust.

[13] 531 SE-ga tunnistatakse kehtetuks AvTS-is olev ISKE määruse volitusnorm.
[14] Vabariigi Valitsuse 20.12.2007 määrus nr 252 „Infosüsteemide turvameetmete süsteem“ (RT I, 15.09.2020, 15).

Lõike eesmärk on sätestada alus teenuse osutajale, kes on andmekogu vastutav töötleja, andmekogude erisuste rakendamiseks turvameetmete rakendamisel ning koondab endas ISKE määruse § 4 lõike 1 ja § 5 lõike 1 regulatiivset sisu.

Lõige 2 kehtestab andmekogu andmetele määratud turvaklassi ja andmekogu turbastme kooskõlastamise korra. Lõige säilitab ISKE määruse § 4 lõike 2 regulatsiooni.

Lõige 3 kehtestab piirangu andmekogude kasutamisele. Nimelt peavad enne või hiljemalt andmekogu kasutusele võtmise ajaks olema rakendatud ka turvameetmed. Samasisuline nõue oli kuni 17.09.2020. a ISKE määruse § 4 lõikes 2.[15] Õigusselguse tagamiseks on vajalik määratleda, mis ajaks on vajalik tagada turvameetmete rakendamine, mistõttu toimub selle sätte uuesti kehtestamine. Kasutusele võtmise aeg on seotud kommenteeritava paragrahvi lõikes 2 viidatud kooskõlastusmenetlusega riigi infosüsteemi haldussüsteemis ehk RIHA.[16] Näiteks uute andmekogude puhul peavad turvameetmed olema rakendatud andmekogu lõpliku registreerimise ajaks (st kui andmekogu saab RIHA-sse märke "kasutusel").

Lõige 4 alusel kehtestatav kohustus turvameetmete rakendamiseks lähtuvalt andmekogu turbeastmele kohaldub teenuse osutajatele, kes on nii andmekogu vastutavad töötlejad kui ka andmekogu majutamiseks volitatud töötlejad. Andmekogu turbeastmest tulenevad turvameetmed lähtuvad E-ITSi rakendamise erikorrast, mis on omakorda reguleeritud eelnõu §-s 11. Lõige säilitab kuni 17.09.2020. a kehtinud ISKE määruse § 4 lõike 2 teise lause regulatsiooni.

Eelnõu § 8 kehtestab andmekogu turbeastme määramise korra. Turbeastme määramine lähtub otseselt andmekogusse kogutavatele andmetele määratud turvaklassi turvaosaklassist. Paragrahviga säilitatakse ISKE määruse § 6 lõike 1 sisu.

Esimene lõige sätestab kolm võimalikku andmekogu turbeastet – kõrge (H), keskmine (M) või madal (L). **Teine lõige** määratleb, kuidas konkreetsetest andmete turvaklassi osaklassidest lähtuvalt andmekogu turbeastet määrata. Andmete turvaklassi määramise korra kehtestab eelnõu § 8 ning turvaosaklasside määramise eelnõu § 9.

Turbeastme määramist on võimalik määratleda järgnevalt:

Andmekogu andmete turvaklassi (KTS) kõrgeima numbrilise väärtusega turvaosaklassi (K, T või S) väärtus	Andmekogu madalaim võimalik turbeaste
0	L
1	L
2	M
3	H

[15] Eelnõude infosüsteemi toimik nr 20-0208: Vabariigi Valitsuse 20. detsembri 2007. a määruse nr 252 „Infosüsteemide turvameetmete süsteem“ muutmine – kättesaadav: https://eelnoud.valitsus.ee/main/mount/docList/0909a3a0-38ed-434c-8dc3-7a9c0f87be92.
[16] Riigi infosüsteemi haldussüsteem ehk RIHA – lisainfo: https://www.riha.ee/Avaleht.

On lubatud määrata andmekogule ka kõrgem turbeaste kui madalaim turbeaste ehk andmete turvaklassi turvaosaklassi väärtusele vastav turbeaste. Kõrgema turbeastme määramine võib kuuluda kohaldamisele, kui rakendaja soovib sõltumata madalamast andmete turvaklassist rakendada andmekogule kõrgemaid küberturvalisuse tagamise nõudeid.

Andmekogu turbeastmete määratlemine on vajalik küberturvalisuse tagamisega seotud edasiste tegevuse jaoks – ennekõike turvameetmete valiku ja rakendamise teostamiseks. Vt siin ka eelnõu §-i 11.

Eelnõu § 9 kehtestab andmekogu andmete turvaklassi määramise korra. Andmete turvaklass on otseselt tuletatud andmete turvaosaklasside numbrilistest väärtustest. Andmete turvaosaklasside määramine kehtestatakse eelnõu § 10 alusel.

Lõiked 2–4 selgitavad erinevate turvaosaklasside (käideldavus, terviklus ja konfidentsiaalsus) tähendusi ning lõige 5 selgitab turvaklassi määramise korda. Kuna andmekogude osas säilitatakse eelnõuga eraldi regulatsioon ning see jõustub erineval ajal eelnõust, siis ei ole mõistlik nimetatud termineid sisustada eelnõu §-s 2.

Lõige 1 säilitab ISKE määruse § 6 lõike 2 sisu. Lõiked 2-4 säilitavad ISKE määruse § 6 lõigete 3-5 sisu. Lõige 5 säilitab ISKE määruse § 3 lg 1 punkti 7 ja § 5 lõike 4 mõtet ning §-i 8 sisu.

Eelnõu § 10 kehtestab andmekogu andmete turvaosaklasside määramise korra.

Lõige 1 sätestab turvaosaklassi mõiste tähenduse. Turvaosaklassil on tähis (K, T või S) ning numbriline väärus (0, 1, 2, 3). Tähis märgistab andmete tagatava parameetri (käideldavus, terviklus või konfidentsiaalsus) ning numbriline väärtus tähistab vastava tagatava parameetri tähtsusest tulenevat infoturbe eesmärki.

Lõige 1 säilitab ISKE määruse § 3 lg 1 punktis 8 olevat termini sisu ning mõtet.

Lõige 2 sätestab alused, millest lähtuvalt tuleb määrata andmete tagatava kvaliteedi infoturbe eesmärke hinnata. Vastavalt lõigetele 3-5 on sätestatud andmete erinevate turvaosaklasside numbrilised väärtused ja sellele vastav infoturbe eesmärk (vajalik saavutatav tulem). Kui turvaosaklass koos tähise ja numbrilise väärtusega vastab konkreetsele saavutatavale infoturbe eesmärgile, siis lõikes 2 on sätestatud alused, millest lähtuvalt peab rakendaja hindama, milline peaks selle andmekvaliteedi osas soovitud infoturbe eesmärk kui vajalik saavutatav tulem. Andmete vastava turvaosaklassi määramiseks on seega vajalik võtta aluseks kolm peamist kriteeriumi.

Esimene kriteerium on andmetega seotud nõuded (nii lepingulised kui ka õigusaktidest tulenevad). Näiteks kui andmekogu töötleb asutusesiseseks kasutamiseks mõeldud teavet, ei saaks olla põhjendatud nendele andmetele konfidentsiaalsuse osaklassi „S0“ määramine.

Teine kriteerium on andmetega seotud pakutavate teenuste iseloom. Näiteks kui andmekogu on kriitiline osa elutähtsa teenuse osutamist tagavast süsteemist, siis ei ole põhjendatud andmete käideldavuse osaklassi „K1“ määramine.

Kolmas kriteerium on küberintsidendist tekkiv kahju. Küberintsidendi all on mõeldud küberintsidenti KüTS § 2 punkti 3 tähenduses. Kriteerium võtab eelduseks, et küberintsident

toimub andmekogu või seda toetava süsteemi suhtes ning selle tulemusena on mõjutatud andmete käideldavus, terviklus või konfidentsiaalsus. Näiteks võib andmekogu küberintsident oluliselt muuta või isegi hävitada karistusregistri andmed. Sellest tekkiv kahju on piisavalt oluline, et ei oleks põhjendatud andmete tervikluse osaklassi „T1“ määramine.

Iga rakendaja ülesanne on hinnata lõikes sätestatud aluste põhjal andmete tähtsust objektiivselt ning kooskõlas KüTS §-s 6 sätestatud küberturvalisuse tagamise põhimõtetega. Erinevatel kriteeriumitel võib konkreetsete andmekogumite osas olla erinev tähtsus. Kui üks kriteeriumitest viitab kõrge väärtusega turvaosaklassi määramisele, siis see võib põhjustada ka vajaduse määrata kõrge väärtusega turvaosaklass sõltumata teiste kriteeriumite viitamistele madalama turvaosaklassi määramiseks.

Lõiked 3-5 kehtestavad iga turvaosaklassi tähise igale numbrilisele väärtusele vastava saavutatava infoturbe eesmärgi taseme ehk turvaosaklasside skaala. Nimetatud lõiked säilitavad ISKE määruse § 7 sisu. Eelnõus säilitatavate sätete osas on tehtud ainult üks erisus võrreldes ISKE määruse § 7 lg 3 punktidega 2-4 – sõnade „õigustatud huvi“ asemel on kasutatud sõna „teadmisvajaduse“. See muudatus ei muuda lause mõtet ning see võimaldab välistada ebaselguse, et nimetatud sõnastused oleksid seotud isikuandmete kaitse üldmääruses[17] sätestatud õigustatud huvi kui ühe isikuandmete töötlemise õigusliku alusega.

Lõige 6 sätestab andmete turvaosaklassi määramise korra juhul, kui andmekogu analüüsitavad andmed on mitmeliigilised (andmestik). Üldjuhul on andmekogudes salvestatud andmed mitmeliigilised, näiteks isikuandmeid puudutavates andmekogudes salvestatakse rohkem kui lihtsalt andmesubjekti nimi (isikukood, andmekoguga seotud teenuse jaoks vajalikud andmed jms). Sellisel juhul lähtutakse andmete (kui terviku) turvaosaklassi määramisel just nendest andmetest, millest tuleneb suurim kaitsevajadus lõikes 2 sätestatud alustel infoturbe eesmärkide määramisel. Siinne lõige säilitab ISKE määruse § 5 lõike 3 sisu.

Eelnõu § 11 kehtestab turvameetmete rakendamise lähtuvalt andmekogu turbeastmest. Eelnõu § 7 lõike 4 alusel on teenuse osutajal kohustus rakendada andmekogu pidamisega seotud süsteemide turvameetmeid andmekogu turbeastmest lähtuvalt. Sisuliselt eeldab selle kohustuse täitmine erisuste rakendamist E-ITS-i järgimisel. Sellest tulenevalt on eelnõus kasutusel ka E-ITS-i spetsiifilised terminid „kaitseala“, „kaitsetarve“, „standardturve“, „väga suur (VS)“, „suur (S)“ ja „normaalne (N)“.

Lõige 1 kehtestab erisuse E-ITS-i tingimuste järgimisel kaitsetarbe ja turbeviisi määramisele. E-ITS-i tingimuste järgi tuleb kaitsetarbe määramisel lähtuda varasemalt määratletud kaitsealast (nt infovarade kogumik). Käesoleva lõike alusel on teenuse osutajal keeld arvestada andmekogu ning selle pidamisega seotud süsteemid erinevatesse kaitsealadesse. Täiendavalt ei saa nimetatud kaitsealale määrata madalamat kui andmekogu turbeastmele vastavat kaitsetarvet. Kaitsetarve (E-ITS) ja turbeaste (ISKE) on sisuliselt sarnased terminid, mis iseloomustavad süsteemide küberturvalisuse tagamise olulisust. Lõikes 2 on kehtestatud ka igale andmekogu turbeastmele vastav andmekogu sisaldava kaitseala kaitsetarve. Kui teenuse

[17] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 04.05.2016, lk 1–88).

osutaja on otsustanud rakendada turvameetmeid vastavalt E-ITS etalonturbe kataloogidele, siis peab teenuse osutaja, sõltumata sellest, kas E-ITS tingimuste järgimisel oleks lubatav ka põhiturbe või tuumikuturbe rakendamine, rakendama standardturbe turveviisi.

Lõige 2 kehtestab igale andmekogu turbeastme väärtusele vastava E-ITS-is kehtestatud kaitsetarbe väärtuse.

Lõige 3 kehtestab erandi andmekogust turbeastmest tulenevate erisuste arvestamisele turvameetmete rakendamisel. Nimelt loetakse eelnõu § 7 lõikes 4 sätestatud kohustus täidetuks, kui teenuse osutaja on täitnud § 3 lõikes 2 sätestatud tingimuse ehk E-ITS-i asemel on rakendanud rahvusvahelise standardiga ISO/IEC 27001 standardile vastavad turvameetmed ning esitanud RIA-le kehtiva vastavussertifikaadi.

Eelnõu §-id 12 ja 13 (3. peatüki 2. jao 2. jaotis) kehtestavad küberturvalisuse nõuete erisused avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamisele. Eesmärk on kindlustada avaliku sektori põhifunktsioonide täitmiseks vajalike andmete turvaline säilitamine ja ligipääs ning elutähtsate infosüsteemide töös hoidmine teenuste osutamiseks ka siis, kui riigi territooriumil asuvate andmekeskuste töö on peatunud või häiritud näiteks looduskatastroofi, ulatusliku küberrünnaku, elektrikatkestuse või muu kriisiolukorra tõttu.

Eelnõu § 12 sätestab kaheteistkümnest kriitilisest süsteemist koosneva loetelu, millel on oluline mõju riigi- ja kohaliku omavalitsuse üksuse asutuse võimele avalikke ülesandeid täita.

Lähtudes MKM-i küberturvalisuse strateegiast 2019-2022 on kõige enam kaitset vajavateks digitaalseteks varadeks põhiandmed kodanike, riigi territooriumi ja õigusloome kohta[18]. Kriitiliste andmekogude töörühm, mis käis koos MKM-i juhatamisel selgitasid välja avalike ülesannete täitmist oluliselt mõjutavad süsteemid, mis on ka küberjulgeoleku nõukogu[19] poolt kinnitatud.

Nendeks kriitilisteks süsteemideks on e-toimiku süsteem, elektrooniline kinnistusraamat, äriregister, riigi- ja kohaliku omavalitsuse asutuste riiklik register, mittetulundusühingute ja sihtasutuste register, kommertspandiregister, Riigi Teataja infosüsteem, elektrooniline kataster, riigikassa infosüsteem, maksukohustuslaste register, rahvastikuregister, sotsiaalkaitse infosüsteem. Eelnõus on kasutatud nimetatud andmekogude ametlikke nimetusi, mis on nimetatud vastavat andmekogu reguleerivas seaduses või põhimääruses.

Eelnõu § 13 sätestab §-s 12 loetletud süsteemide varundamise nõuded.

Paragrahv sätestab, et süsteemide andmekoosseis tuleb varundada välisriigi andmekeskusesse (edaspidi *andmesaatkond*), vajadusel koos andmekoosseisu kasutamiseks vajaliku toimiva rakenduskihiga.

---

[18] Majandus- ja Kommunikatsiooniministeerium. Küberturvalisuse strateegia 2019-2022, lk 24. Kättesaadav: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf.

[19] 2009. aastal alustas Vabariigi Valitsuse julgeolekukomisjoni juures tööd küberjulgeoleku nõukogu, mille ülesanne on aidata kaasa ametkondade koostöö toimimisele ja teha järelevalvet küberjulgeoleku strateegia eesmärkide elluviimise üle. Nõukogu esimees on ettevõtlus- ja infotehnoloogiaminister ning nõukogu juhib MKM-i kantsler.

Andmed varundatakse rahvusvahelise lepingu alusel andmesaatkonda tagamaks, et olukorras, kus riigi territooriumil asuvate andmekeskuste töö on peatunud või häiritud näiteks sõja, looduskatastroofi, ulatusliku küberrünnaku, elektrikatkestuse või muu kriisiolukorra tõttu, riigi ja kohaliku omavalitsuse üksuse asutuste põhifunktsioonide täitmiseks vajalikud andmed ei hävineks; tagatud oleks nende kestev säilimine ning neid oleks võimalik võtta kasutusse kas koheselt, ilma, et elutähtsa teenuse osutamine ebaproportsionaalselt pikaks ajaks peatuks või lõppeks või hiljem, kui tekib taas võimalus andmete baasil avalike ülesandeid täita. Teisisõnu on andmesaatkonna pidamise eesmärk tagada Eesti omariikluse ja digitaalse järjepidevuse säilimine läbi oluliste andmete tervikluse, käideldavuse ja konfidentsiaalsuse tagamise.

Selleks, et andmesaatkonda varundatud andmekoosseise oleks võimalik realiseerida (varukoopiate alusel andmekoosseisud taastada), on vajalik, et lisaks andmekoosseisudele oleks andmesaatkonda varundatud ka vastavate infosüsteemide rakenduskiht ja muu, mis on vajalik andmete kasutuselevõtuks ja elutähtsate teenuste toimimiseks. Näiteks saab varundada koopia virtuaalmasinast või andmekogu koos selle info- ja tootesüsteemiga. Pelgalt andmebaasi sisu ehk andmete ning sellega seonduva tarkvara lähtekoodi varundamine ei võimalda efektiivselt andmesaatkonda varundatud andmeid taastada, kui selleks peaks vajadus tekkima. Andmekoosseisu varundav asutus hindab läbi testimise, kas välisriigi andmekeskusesse varundatud süsteemi on võimalik töösse rakendada kasutades ainult varundatud faile.

Kommenteeritav paragrahv ei tähenda, et mõne riigiga tuleb sõlmida rahvusvaheline leping, vaid see selgitab, et kui see on sõlmitud, siis andmete vahetamine toimubki selle lepingu alusel. Lisaks sellele lepingule võikase ette näha seda lepinguid täiendavaid kokkuleppeid – nt võidakse leppida kokku varundamisega seotud üksikasjad Eesti Vabariigi ja välisriigi vahelise andmete ja süsteemide majutamise kokkuleppega.

Kuivõrd andmesaatkonna kontseptsioon on uudne ning tegemist ei ole vaatamata mitteametlikule nimetusele „andmesaatkond“ siiski diplomaatilise esindusega, millele kohaldatakse diplomaatiliste suhete Viini konventsioonist[20] tulenevalt välisesindustele omaseid eesõigusi ja puudutumatust, on vajalik sõlmida rahvusvaheline leping, mille eesmärgiks on kaitsta Eesti riigi avalike ülesannete täitmist oluliselt mõjutavaid süsteeme ja nendes sisalduvate andmete puutumatust ning tagada neile välisesindustega sarnane kaitse. Riikidevaheline kokkulepe määrab kindlaks riikide kohustused ja õigused, mis on vajalikud Eesti riigi andmete ja süsteemide kaitsmiseks.[21]

Eelnõu §-id 14 kuni 19 (3. peatüki 2. jao 3. jaotis) kehtestavad küberturvalisuse nõuete erisused pilvsüsteemide pidamisel. Pilvsüsteem on käesolevas määruses defineeritud süsteemi eriliik. Käesolevas jaotises sätestatud nõuete eesmärk on luua regulatiivne raamistik avalikule sektorile pilveteenuste kasutamiseks avalike ülesannete täitmisel. Pilveteenuste kasutamise ajendiks on ennekõike majanduslikud eelised andmetöötlusressursside kasutamiseks vastavalt kasutaja vajadusele, kuid kasutamisega kaasnev olemuslik risk on tehnilise kontrolli puudumine kasutatava infrastruktuuri üle. Regulatiivse raamistiku puudumisel võib seega tekkida liigne risk avaliku sektori toimepidevusele, kui pilvandmetöötlusteenuste majanduslikke eeliste

[20] Diplomaatiliste suhete Viini konventsioon; välisleping avaldatud RT II 2006, 16.
[21] Eesti Vabariigi ja Luksemburgi Suurhertsogiriigi vahelise andmete ja infosüsteemide majutamise kokkuleppe ratifitseerimise seadus 563 SE seletuskiri. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/.

kõrval puudub kohustus ka teenusega seotud riskide hindamiseks. Sätted kehtestavad seega põhilised eeltingimused, mille eesmärk on kaasnevat riski või selle mõju vähendada süsteemide osas, mis on vajalikud avalike ülesannete täitmiseks. Sellest tulenevalt on käesoleva jaotise sätetel kaks iseärasust.

Esimene paragrahv on kohaldamisala. Käesoleva jaotise sätteid kohaldatakse vaid osale KüTS-i kohaldamisalast – avalikule sektorile. Teine on turvameetmete erinõuete iseloom. Ennekõike on tegemist protseduuriliste nõuetega pilvsüsteemi pidamisel, mida rakendatakse kasutatava pilvandmetöötlusteenuse valimiseks, mitte tehniliste nõuetega pilvsüsteemile endale.

Jaotises on sätestatud KüTS § 7 lõike 1 struktuuri eeskujul pilvsüsteemi pidamisele rakendatavate turvameetmete erinõuded vastavalt nõude eesmärgile kas küberintsidendi ennetamiseks, lahendamiseks või selle mõju leevendamiseks.

Eelnõu § 14 sätestab nõuete kohaldamise ulatuse. Olulisim on teises lõikes sätestatu, mis kitsendab jaotise nõuete kohaldamisala konkreetsele osale KüTS-i subjektidest. Pilvsüsteemide pidamisega seotud nõudeid kohaldatakse vaid KüTS § 3 lõikes 4 sätestatud loetelule. Eelnõu koostamise hetkel on selleks loeteluks:

1) andmekogu vastutav töötleja ning volitatud töötleja;
2) Arenguseire Keskus;
3) Eesti Pank;
4) kohaliku omavalitsuse üksus ja kohaliku omavalitsuse üksuste liit;
5) kohtuasutus;
6) riigi valimisteenistus;
7) Riigikogu Kantselei;
8) Riigikogus esindatud erakond;
9) Riigikontroll;
10) Riigimetsa Majandamise Keskus;
11) seaduse alusel asutatud avalik-õiguslik juriidiline isik;
12) Vabariigi Presidendi Kantselei;
13) valitsusasutus ja valitsusasutuse hallatav riigiasutus;
14) valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavald ning linnaosa, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus, omavalitsusüksuste ühisamet ja -asutus;
15) Õiguskantsleri Kantselei.

Eelnevalt toodud loetelu lisandub KüTS-i 531 SE tulemusena.

Käesolevas jaotises on toodud loetelu ühisnimetajaks määratud „kasutaja“, viitamaks asjaolule, et KüTS-i subjekt kasutab pilvsüsteemi pidamiseks pilvandmetöötlusteenust. Tegemist on nn avaliku sektori loetelu osaga KüTS subjektide laiemast loetelust. Kuivõrd jaotises loodav regulatiivne raamistik mõjutab subjekti majanduslikku käitumist pilvandmetöötlusteenuste soetamisel, siis on eesmärk rakendada eelkirjeldatud riske maandavat raamistikku avaliku sektori süsteemidele vähemalt kuni pole hinnatud, kas vastav raamistik on eesmärgipärane ning vajalik regulatsioon ka KüTS erasektori subjektidele.

Kuivõrd jaotis on erineva kohaldamisalaga muu eelnõuga kehtestatava määruse või selle alusel kehtestatud nõuete kohaldamisalaga võrreldes, on olemas ka võimalus regulatiivsete erisuste tekkimiseks käesoleva jaotise ja muude sätete vahel. Sellest tulenevalt on paragrahvi esimeses lõikes sätestatud, et vastuolude korral kohaldatakse käesoleva jaotise sätteid. Ennekõike võib vastuolu tekkida selle määruse alusel kehtestatavate E-ITS-i nõuetega, mis võivad sätestada etalonturbe meetmete nõudeid arvestamata käesoleva raamistiku erisusi. Käesoleva eelnõu koostamise hetkel eelnõuga sätestatavate nõuete ja E-ITS-i nõuete vahel ühtegi vastuolu tuvastatud ei ole. E-ITS nõudeid rakendatakse lisaks raamistikule ning on oluline välja tuua, et ka vastuolu korral kohaldatakse kõiki nõudeid osas, mis ei ole vastuolus. Lisaks E-ITS-le tuleb ka arvestada võimalusega, et kasutaja võtab E-ITS-i asemel kasutusele ISO/IEC 27001 – sel juhul tuleb kasutajal samuti lähtuda siinses jaotises toodud nõuetest.

Eelnõu § 15 sätestab volituse küberturvalisuse korraldamise eest vastutavale ministrile kehtestada määrusega pilvsüsteemi pidamiseks kasutatava pilvandmetöötlusteenuse kohustuslikud tehnilised suvandid. Tegemist on piiritletud pilvandmetöötlusteenuste (näiteks Microsoft 365) kasutamise korra kehtestamisega. Tehnilised suvandid tähendavad kohustuslikke juhiseid kasutajale ennekõike selles osas, et missuguseid valikuid ja teenuse kasutamisega seotud rakenduslikke tegevusi peab kasutaja selle pilvandmetöötluse kasutamisel tegema. Sätte eesmärk on ennetada levinumate pilvandmetöötlusteenuste kasutamisega seotud riske kasutaja pilvsüsteemi turvalisusele, mis võivad tuleneda kasutaja (kui organisatsiooni) vähesest tehnilisest pädevusest või hooletusvigadest teenuste seadistamisel.

Eelnõu § 16 kehtestab pilvandmetöötlusteenuse pakkujast kui organisatsioonist tuleneva riski hindamise kohustuse.

Kui süsteem viiakse „pilve“ ehk kui peetakse süsteemi pilvsüsteemina, mõjutab selle pilvsüsteemi turvalisust suuresti kasutatav pilvandmetöötlusteenus. Pilvsüsteemi turvalisus tähendab muidugi KüTS § 2 lõikes 2 sätestatud süsteemi turvalisuse mõistet kohandatuna pilvsüsteemile ehk süsteemile, mille pidamist teostab kasutaja pilvandmetöötlusteenust kasutades. Kasutajal on aga praktikas keeruline hinnata kasutatava pilvandmetöötlusteenuse turvalisust, seda ennekõike kasutatava tehnoloogilise lahenduse kasvava keerukuse, läbipaistmatuse ning hindamiseks vajaliku tööjõu puudumise tõttu. Suuremate tehniliste puuduste või turvariskide tuvastamine ehk üldine kvaliteedihindamine on kindlasti võimalik, kuid oluline keerukus seisneb just peidetud riskide tuvastamises või nende olemasolu objektiivses välistamises. Siiski ei mineta see takistus vajadust pilvsüsteeme kaitsta ehk näiteks vältida avaliku sektori süsteemide sidumist pilvandmetöötlusteenustega, mis selle turvalisust ohustavad.

Pilvandmetöötlusteenuse tehnilise lahenduse hindamise kõrval on aga lihtsamini võimalik hinnata seda teenust pakkuvat organisatsiooni ehk pilvandmetöötlusteenuse pakkujat. Pakkujast tulenevate riskide hindamine võimaldab kasutajal välistada suurel määral riske pilvsüsteemi turvalisusele, mille tuvastamine väljuks muidu lahenduse üldise kvaliteedihindamise ulatusest, sest pilvandmetöötlusteenuse puhul mõjutab pilvsüsteemi turvalisust kestvuslepingulisele suhtele iseloomulikult ka pakkuja tegevus teenuse osutamisel ning siin ongi peamiseks kriteeriumiks pakkuja usaldusväärsus kasutajale.

Käesoleva paragrahviga loodav pilvandmetöötlusteenuse pakkujast tuleneva riskihindamise raamistik ei jõua seega järelduseni pilveandmetöötlusteenuse tehnilise turvalisuse osas, vaid jõuab hinnanguni süsteemi turvalisust ohustavate riskide esinemise ning peitmise tõenäosuse suhtes teenuse osutamisel pilvandmetöötlusteenuse pakkujast kui organisatsioonist tulenevalt.

Raamistik on sisult hinnanguline ning hinnangu annab kasutaja. Keelatud on kasutada pilveandmetöötlusteenust, mille pakkujast tuleneb kõrge risk pilvsüsteemi turvalisusele, seega ei ole hindamise küsimus selles, et kas kasutaja leiab ükskõik millise riski pilvsüsteemi turvalisusele pakkuja organisatsioonist tulenevalt, vaid kas leitav on kõrge risk. Kuivõrd siinkohal ei vaadelda pilvandmetöötlusteenuse kasutamise eesmärki, siis ei ole kõrge risk seotud kahjuliku tagajärje ulatusega. Käesolevas raamistikus on riski väärtus seotud riski tõenäosusega ehk risk on kõrge sellisel juhul, kui on tõenäoline, et pakkujast kui organisatsioonist tulenevalt, kaasnevad tema pilvandmetöötlusteenuse kasutamisega riskid, tehniliselt peidetud või mitte, pilvsüsteemi turvalisusele. Pakkujast tulenev risk tähendab siinkohal, et pakkuja hindamisel on tuvastatud ebausaldusväärsusele viitavad asjaolud või pole suudetud saada teavet, mis pakkuja usaldusväärsust hinnata võimaldaksid.

Suur osa avalikus sektoris kasutatavatest pilvandmetöötlusteenustest pakuvad loetletud teenusepakkujad. Kuivõrd teenusepakkuja hindamine tugineb rangelt organisatsiooni enda hindamisele ning ei lähtu konkreetsest teenusest, selle olulisusest kasutajale ega ka teenuse kasutamise eesmärgist, ei ole kuidagi välistatud võimalus kasutajal tugineda mõne teise kasutaja riskihinnangu järeldustele. Samas ei võta teise kasutaja riskihinnangule tuginemine ära kasutaja enda vastutust kohustuse asjakohase täitmise üle.

MKM-l on kavas levinumate teenusepakkujate suhtes korduvate riskihindamiste tegemise halduskoormuse vähendamiseks luua keskne riskihindamise mehhanism, mille kaudu avalikustataks riskihinnangud levinumate teenusepakkujate suhtes. Variante riskihindamisi teostavateks asutajataks on mitmeid, näiteks muutub üheks suurimaks pilveandmetöötlusteenuste kasutajaks Riigi Info- ja Kommunikatsioonitehnoloogia Keskus (edaspidi RIT). Samuti saab RIA teha korrakaitseseaduse[22] alusel ohuhinnanguid konkreetse pilveteenuse osutaja suhtes, arvestades siinses paragrahvis olevaid sätteid. Samalaadset analüüsi saab teha ka IT-maja ning selle analüüsi ise avalikustada osas, mis pole juurdepääsupiiranguga.

Lõige 1 sätestab kasutajale kohustuse lähtuda pilvsüsteemide pidamisel selliste pakkujate teenustest, kellest ei tulene kõrget riski pilvsüsteemi turvalisusele. Lisaks ülaltoodule on vajalik selle lõike all ka täpsustada, et sätestatud kohustus on ajaliselt kestev. Praktikas on seega kasutajal vajalik olla kursis pilvandmetöötlusteenuse pakkuja kui organisatsiooniga jooksvalt, sest olulised muutused pakkuja organisatsioonis võivad tõstatada vajaduse riskihindamise ajakohastamiseks, kuivõrd varasema hindamise eeldused on muutunud.

Lõige 2 sätestab esimeses lõikes sätestatud kohustuse järgimise tagamiseks pakkuja suhtes riskihindamise läbiviimise kohustuse. Kui kasutaja soetab pilvandmetöötlusteenust läbi hankemenetluse, tuleb kasutajal hanget korraldades tähelepanu pöörata käesoleva nõude täitmisele pakkujate suhtes. Kui hankija ei sätesta piisavaid nõudeid pakkujatele hanke

[22] Korrakaitseseadus, RT I, 03.03.2021, 5.

korraldamisel, võib ta sattuda käesoleva paragrahvi lõikes 1 sätestatud kohustuse rikkumisse, kui sõlmib hanke tulemusena lepingu kõrge riskiga (pilveteenuse) pakkujaga.

Lõikes 3 esitatakse näitlik loetelu, millist teavet pilvandmetöötlusteenuse pakkujast tuleneva kõrge riski hindamisel muu hulgas arvestatakse ning mis võib ohustada pilvsüsteemi turvalisust. Loetelu põhineb analoogsetel kriteeriumitel, mida rakendatakse sidevõrgus kasutatava riist- või tarkvara tootja või hooldus- või tugiteenuse pakkujast tuleneva riski hindamisel elektroonilise side seaduse § 87^3 lõike 3 alusel.[23]

Loetelu ei tähenda, et kui üks tingimus on täidetud, oleks tegu automaatselt kõrge riskiga pakkujaga. Käesolevas raamistikus on riski väärtus seotud riski tõenäosusega ehk risk on kõrge sellisel juhul, kui on tõenäoline, et pilveandmetöötlusteenuse pakkujast kui organisatsioonist tulenevalt, kaasnevad tema pilvandmetöötlusteenuse kasutamisega riskid, tehniliselt peidetud või mitte, pilvsüsteemi turvalisusele. Ühe loetelus nimetatud punkti täitmine võib põhimõtteliselt kaasa tuua kõrge riski, kuid eeldusel, et see on piisavalt kaalukas.

Punktid, mida pilvandmetöötlusteenuse pakkuja kohta riskianalüüsis muu hulgas hinnatakse, on tema asukohariik (täpsemalt pakkujale kohalduva jurisdiktsiooni sobivus demokraatliku õigusriigi avaliku sektori süsteemide pidamiseks) (1-8), äritegevus (8-10), käitumine teenuste turvalisuse või toimepidevuse tagamisel (11-12) ning pakkuja kasutatava tarneahela vastavus loetletud punktidele (13).

Punktid 1-8 hindavad ennekõike seda, kas pakkujale kohalduv jurisdiktsiooni on sobiv demokraatliku õigusriigi avaliku sektori süsteemide sidumiseks nende pilvandmetöötlusteenustega.

Eesti on Euroopa Liidu, NATO ja OECD liikmesriik. Nende organisatsioonide liikmesriikides asuvad ettevõtjad on üldiselt vähem riskantsed, kuna nendes riikides kehtivad kokkulepped, väärtused ja põhimõtted, mis ühilduvad Eesti riigi julgeoleku huvidega. OECD liikmesriike ühendavad väärtused nagu avatud turumajandus, demokraatlik pluralism ja inimõiguste austamine ning NATO liikmesriike isikute vabadus, demokraatia, inimõigused ja õigusriik. Euroopa Liidu põhimõtted on inimõiguste austamine, demokraatia, õigusriik, inimväärikus, vabadus ning muud Euroopa Liidu õigusaktides sätestatud põhimõtted. Neid väärtusi kandvad riigid on üldiselt vähem tõenäolised sekkuma oma riigis asuva ettevõtja tegevusse eesmärgiga kahjustada Eesti riigi julgeolekut.

Sarnaselt eeltooduga on väiksem risk taolisele sekkumisele, kui asukohariigis järgitakse demokraatliku õigusriigi põhimõtteid ja austatakse inimõigusi ning kaitstakse muu riigi isikute intellektuaalomandit, isikuandmeid ja ärisaladust.

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

[23] Elektroonilise side seadus, RT I, 27.02.2022, 3.

Riik, kus kaitstakse muu riigi isikute intellektuaalomandit, isikuandmeid ja ärisaladust, on vähem tõenäoline sekkuma enda riigis asuva ettevõtja tegevusse eesmärgiga teise riigi isikute intellektuaalomandit, isikuandmeid või ärisaladust rikkuda. Kuna pilvsüsteemid võivad olla riigi ja ühiskonna toimimisel olulise tähtsusega ning töötlevad suures koguses andmeid (sh isikuandmeid või juurdepääsupiiranguga andmeid), siis peab olema kindlus, et pilvsüsteemidele nende pidamiseks kasutatavate pilvandmetöötlusteenuste kaudu kolmandatel isikutel ja riikidel õigusvastaselt juurdepääsu pole.

Teave, et asukohariik käitub küberruumis agressiivselt või Euroopa Liidu, NATO või OECD liikmesriigid on asukohariigile omistanud küberrünnakuid, viitab, et asukohariik võib taolisi küberrünnakuid korraldada pilvandmetöötlusteenuste tehnoloogia kaudu ka Eesti vastu.

Punktid selle kohta, kas ettevõtja allub sõltumatu kohtuliku kontrollita asukohariigi või muu välisriigi valitsusele või riigiasutusel ning kas tema asukohariik või muu välisriik võib kohustada teda tegutsema Eesti riigi julgeolekut ohustaval viisil, baseeruvad eelkõige teise riigi õigusruumi hindamisel. Kui näiteks asukohariigi õigusaktid võimaldavad kohtuliku kontrollita anda ettevõtjale korraldusi luure või riigikaitse huvides teise riigi järele luurata, on see ohumärk Eesti riigi julgeoleku aspektist.

Punktid 8-10 hindavad eelkõige seda, kas ettevõtjal võib olla varjatud sidemeid välisriigi valitsusega, mis panevad teda sõltuma selle välisriigi valitsuse tahtest ning luure ja agressiivse teiste riikide mõjutamise kaalutlustest.

Punktid 11-12 keskenduvad eelkõige sellele, kas pilveandmetöötlusteenuse pakkuja ise tähtsustab küberturvalisust ning on suuteline tarneid tagama. Kui ettevõtja ise küberturvalisust ei tähtsusta, on suurem risk, et tema riist- ja tarkvara sisaldab ohtlikke turvanõrkusi. Kui ettevõtja järjepidevalt, ka pahatahtlikult, teenuste toimepidevust ei taga, seab see ohtu pilvsüsteemi toimimise ja turvalisuse.

Punkt 13 sätestab, et lisaks pakkujale tuleb hinnata ning kontrollida pilvandmetöötlusteenuse pakkujaid, keda hinnatav organisatsioon ise teenuse pakkumiseks kasutab. Pilvandmetöötlusteenused võivad tihti tugineda teistele pilvandmetöötlusteenustele, tüüpiliselt näiteks ühe teenusepakkuja IaaS/PaaS lahendusel tugineva PaaS/SaaS lahenduse pakkumine kasutajale. Sellistes olukordades ei tohiks kasutaja pimesi usaldada oma teenusepakkuja tarneahelat. Näiteks hiljutine SolarWinds Orion'i intsident näitab, et ka tarneahelas olevatele ohtudele tuleb tähelepanu pöörata.[24] Veel problemaatilised võivad olla aga olukorrad, kus pilveandmetöötlusteenuse pakkujateks on juriidilised kehad, mis on loodud lihtsalt teenuse vahendamiseks ebausaldusväärse lõpliku teenusepakkuja poolt. Üldiselt on teenusepakkujate koostööpartnerid või lahenduse pakkumiseks kasutatavad platvormid pilveandmetöötlusteenuse pakkuja enda poolt avalikustatud. Kui see nii ei ole, siis peab aga kasutaja vastavat teavet pilvandmetöötlusteenuse soetamisel küsima.

Lisaks eeltoodud tingimustele tuleb pilvandmetöötlusteenuse pakkuja valikul arvestada ka muudest õigusaktidest või korraldustest tulenevaid nõudeid – näiteks:

[24] Lisainfo: https://www.solarwinds.com/securityadvisory ning https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/.

- Tuleb arvestada ning lähtuda isikuandmete kaitse valdkonnas kehtivatest nõuetest (näiteks isikuandmete turvalisuse kui ka isikuandmete andmekaitse mõttes kolmandatesse riikidesse edastamise kontekstis).[25]
- Tuleb arvestada ka Euroopa Liidu määratud sanktsioonidega.[26] Lisaks võidakse rahvusvahelise sanktsiooni seaduse[27] alusel välistada teatavate riikide ettevõtete kaupade (või teenuste) kasutamine riigihangetes.[28]

Eelnõu § 17 kehtestab piirangud pilvsüsteemis töödeldava teabe käitlemisele konfidentsiaalsuse tagamise eesmärkidel. Kuigi eelnõu §-s 16 sätestatud raamistik maandab suurel määral pilvandmetöötlusteenuse kasutamisega kaasnevat riski pilvsüsteemis töödeldava avaliku sektori teabe lekkimisele või ärakasutamisele teenusepakkuja poolt, siis ei ole kindlasti usaldusväärsuse hindamise tagajärjel selline risk täielikult maandatud, arvestades, et kasutaja siiski jagab andmete juurdepääsu teenusepakkujaga.

Pilvandmetöötlusteenuse osutamise seisukohast ei tohiks teenusepakkujal olla huvi pilvsüsteemis töödeldavate andmete sisule, sest see teadmine ei ole teenuse osutamiseks vajalik. Seega on enamikel juhtudel usaldusvääruse hindamise järgne jääkrisk andmete lekkimisele või ärakasutamisele piisavalt madal ehk aktsepteeritav.

Teatud avaliku sektori poolt töödeldavate andmete puhul on aga andmete lekkimise või ärakasutamise tagajärjed oluliselt suurema mõjuga riiklikule julgeolekule. Selles ulatuses jääkrisk vastuvõetavaks ei muutu. Kasutaja poolt pilvsüsteemis töödeldavate andmete liikidest võib eelmainitud mõjuga olla ennekõike asutusesiseseks kasutamiseks tunnistatud teave AvTS tähenduses (edaspidi *AK teave*). Seega tuleb tagada, et kui kasutaja edastab pilvsüsteemi sellist AK teavet, mille lekkimise või ärakasutamise tagajärjed võivad mõjutada riiklikku julgeolekut, oleks ka nimetatud teabe konfidentsiaalsus täiendavalt kaitstud.

Kuivõrd pilvandmetöötlusteenuse osutamise eelduseks ei ole, et pilvandmetöötlusteenuse pakkujale on teada pilvsüsteemis töödeldava teabe sisu, siis on selgeim meede sellise AK teabe lekkimise või ärakasutamise vältimiseks teenusepakkujast tulenevalt tagada teabe konfidentsiaalsus kasutaja poolt ka teenusepakkuja vastu. Selline meede välistaks teenusepakkujast tuleneva riski andmete konfidentsiaalsusele. Praktikas tähendab selline nõue vastava teabe osas ka pilvandmetöötlusteenuse kasutamise eeliste vähenemist, sest paljud pilvandmetöötlusteenuse funktsioonid rakendavad tulemuste saavutamiseks pilvsüsteemis hoitavate andmete automatiseeritud töötlemist. Pilvandmetöötlusteenused oleksid sellise teabe

[25] Kolmandatesse riikidesse isikuandmete edastamise osas lisainfo leitav siit: https://www.aki.ee/et/teenused-poordumisvormid/andmete-edastamine-valisriiki ning Euroopa Andmekaitsenõukogu võrgulehel (https://edpb.europa.eu/our-work-tools/documents/our-documents_et; lehel oleva parempoolses filtreeringus märkida linnuke teema „International transfers of Data“ juurde).

[26] Vt lähemalt https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/what-are-restrictive-measures-sanctions_et ning eraldi vt Venemaa sõjalise agressiooniga seotud sanktsioone siit: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions/sanctions-adopted-following-russias-military-aggression-against-ukraine_en.

[27] Rahvusvahelise sanktsiooni seadus, RT I, 08.03.2022, 3.

[28] Vt ka: Rahandusministeeriumi juhend: kuidas välistada riigihangetes Vene ja Valgevene kaupu ja ettevõtjaid – kättesaadav: https://www.fin.ee/uudised/rm-juhend-kuidas-valistada-riigihangetes-vene-ja-valgevene-kaupu-ja-ettevotjaid.

puhul kõige selgemalt kasutatavad teabe hoiustamiseks ja edastamiseks, kuigi teoreetiliselt ei oleks välistatud ka muud funktsionaalsused.

AvTS-st tulenevalt peab küll teabevaldaja tagama AK teabe konfidentsiaalsuse kolmandate osapoolte eest, kuid AvTS § 38 lõike 4 alusel võib kasutaja lubada kaalutlusotsuse alusel kolmandate isikute juurdepääsu AK teabele. Käesoleva paragrahvi regulatiivne efekt on seega ennekõike nimetatud diskretsiooni nulli viimine riiklikku julgeolekut mõjutava AK teabe osas pilvandmetöötlusteenuse pakkuja suhtes pilvandmetöötlusteenuse pakkumise kontekstis. Täiendavalt sätestab käesolev paragrahv kohustuste tehnilise meetme rakendamiseks samal eesmärgil ehk nimetatud AK teabe krüpteerimise pilvandmetöötlusteenuse pakkuja suhtes.

Lõige 1 kehtestab kasutajale kohustuse lõikes loeteletud teabe konfidentsiaalsus tagada pilvandmetöötlusteenuse pakkuja eest pilvsüsteemis, sealhulgas rakendada tehnilist meedet vastava teabe krüpteerimiseks teenusepakkuja eest. Lõikes on loeteletud AvTS § 35 lõike 1 punktides 3^1, 4, 5, 5^1, 5^2, 6, 6^1, 6^2, 9 või 18^1 sätestatud teave ehk:

1) teave sisejulgeoleku tagamise, riigikaitsepoliitika kujundamise, riigikaitse korraldamise, sealhulgas riigi sõjalise kaitse planeerimise, ettevalmistamise ja juhtimise, või riigisaladuse ja salastatud välisteabe kaitse korraldamisega tegeleva teabevaldaja struktuuriüksuse ülesannete ja koosseisu, ametniku ja töötaja ning tema ülesannete kohta, kui sellise teabe avalikuks tulek ohustaks riigi julgeolekut või riigisaladuse ja salastatud välisteabe kaitset;

2) teave kaitseväe relvastuse ja varustuse tabelite ning relvastuse ja varustuse hulga kohta, kui selline teave ei ole riigisaladus või salastatud välisteave;

3) kaitseväe valdusse sõjalise valmisoleku tõstmisel ja mobilisatsiooni korral üleantava riigivara kohta käiva teave;

4) teave uurimisasutuse tegevuse meetodite ja taktika kohta, kui selle avalikuks tulek võib raskendada süütegude avastamist või soodustada nende toimepanemist;

5) teave politsei relvastuse hulga kohta, kui selline teave ei ole riigisaladus või salastatud välisteave;

6) teave riigikaitselise sundkoormise kohta;

7) teave, mille avalikuks tulek ohustaks riigikaitseobjekti või lihtsustaks selle vastase ründe toimepanemist;

8) teave riigikaitseülesannete täitmiseks ja hädaolukorra tagajärgede leevendamiseks vajaliku varu suuruse ja vahendite koguse kohta ning selle kasutusele võtmise ulatuse ja tingimuste kohta;

9) teabe turvasüsteemide, turvaorganisatsiooni või turvameetmete kirjelduse kohta;

10) elutähtsa teenuse riskianalüüsi ja toimepidevuse plaani puudutav teave.

Loetletud teabeliikide konfidentsiaalsusel on selge seos riikliku julgeolekuga. Teabe loetelu määratluse aluseks on eelkirjeldatud kahjulike riskide maandamise ning pilvandmetöötlusteenuste kasutamise eeliste omavaheline tasakaalustamine. Seega on tegemist

teabeliikidega, mida valdav osa kasutajaid ei töötle või töötleb kontekstis, milleks pilvsüsteemi kasutamine ei ole tingimata vajalik.

Tehnilise meetmena tähendab AK teabe krüpteerimise nõude täitmine ennekõike seda, et kasutaja on muutnud AK teabe teenusepakkujale loetamatuks ning et teenusepakkujal puudub ligipääs võtmele sellise teabe dekrüpteerimiseks ehk loetavaks muutmisele. Krüpteerimiseks kasutatavad materjalid peavad olema piisavalt keerukad, et ka mõistliku pingutuse korral ei oleks eeldatav, et teenusepakkuja suudab dekrüpteerimisvõtit kasutamata teavet dekrüpteerida. Sellise tehnilise meetme täpsemad nõuete kehtestamiseks on käesoleva paragrahvi kolmandas lõikes sätestatud ka volitusnorm.

Eeltoodud nimekirjas ei ole kõik olemasolevad AK alused.[29] Seetõttu eelnõu koostajad märgivad, et siinses lõikes toodud loetelu on esmane loetelu ning aja jooksul võib siia lisanduda ka muid või uusi juurdepääsupiirangute aluseid, kui vastav vajadus peaks tekkima.

Lõikes 2 sätestatakse erand esimeses lõikes kehtestatud piirangule. Teise lõike eesmärk on võimaldada selliste pilvandmetöötlusteenuste eesmärgipärast kasutamist, mis pakuvad kasutajale süsteemide turvalisuse tagamise teenuseid. Tuntud ka kui *security as a service* (SECaaS), on siinkohal tegemist teenustega, mis vajavad ligipääsu süsteemide turvalisusega seotud logide andmetele. Ei ole õiguslikult lõplikult selge, kas AvTS § 35 lõikes 1 punktis 9 sätestatud teave turvasüsteemide, turvaorganisatsiooni või turvameetmete kirjelduse kohta hõlmab määratluse kohaselt ka võrgu- ja infosüsteemi kasutamisega seotud logisid või piirdub traditsioonilisemas vormis dokumentatsiooniga. Turvameetmete teavet, mida sellisel pilvandmetöötlusteenusel toimimiseks vaja ei ole, ei tohiks olla ka pilvandmetöötlusteenuse pakkujale ligipääsetav. Erand rakendub õigusselguse tagamiseks SECaaS lahenduste toimimiseks vajaliku teabe suhtes.

Lõige 3 sätestab volitusnormi lõikes 1 nimetatud teabe krüpteerimise krüptomaterjalide täpsemate tehniliste nõuete kehtestamiseks ministri määrusega. Krüptomaterjalide mõiste tuleneb riigisaladuse ja salastatud välisteabe seadusest ning on täpsemalt määratletud kaitseministri 28.10.2015 määruses nr 29 „Nõuded krüptomaterjalidele, nende töötlemisele ja kaitsmisele.“[30]

Volitusnormi alusel kehtestatud nõuete korral peab kasutaja tagama lõikes 1 nimetatud teabe krüpteerimise pilvandmetöötlusteenuse pakkuja suhtes vähemalt sätestatud tehnilistele nõuetele vastavalt. Osas, kus käesoleva lõike alusel nõudeid kehtestatud ei ole, peab kasutaja tagama lõikes 1 nimetatud teabe krüpteerimise pilvandmetöötlusteenuse pakkuja suhtes vastavalt üldpõhimõttele, et krüpteerimiseks kasutatavad materjalid peavad olema piisavalt keerukad, et ka mõistliku pingutuse korral ei oleks eeldatav, et teenusepakkuja suudab dekrüpteerimisvõtit kasutamata teavet dekrüpteerida.

[29] Vt ka RIHA varamus asuvat juurdepääsupiirangute klassifikaatorit – kättesaadav: https://varamu.riha.ee/#Juurdepaasupiirangute_klassifikaator.
[30] Kaitseministri 28.10.2015 määrus nr 29 „Nõuded krüptomaterjalidele, nende töötlemisele ja kaitsmisele“, RT I, 28.06.2017, 48.

Lõike eesmärk on vajaduse korral võimaldada ühtlase tehnilise lävendiga krüpteerimisnõuete korraldamist ning tagada vajadusel õigusselgus nõuete täitmiseks vajalike tehniliste meetmete suhtes.

Eelnõu § 18 kehtestab kohustuse pilvandmetöötlusteenuste kasutamisel ka teenuse kasutamisega kaasnevate logide edastamiseks RIA-le.

Avalike ülesannete täitmiseks vajalike süsteemide turvalisus on ühiskondlikult olulise tähtsusega, sõltumata sellest, kas süsteem tugineb kasutaja enda infrastruktuurile või peab kasutaja seda pilvsüsteemina. Üks olulisemaid tehnilisi vahendeid süsteemide turvalisuse tagamisel on süsteemis tehtavate toimingute, täpsemalt nende toimingute logide, seiramine. Logide seiramine võimaldab koheselt tuvastada ebaregulaarseid või volitamata toiminguid süsteemis ning seega ka asuda võimaliku küberintsidendi lahendamisele suuremaid kahjusid ära ootamata.

Paljudele avalikus sektoris kasutatavatele süsteemidele teeb aktiivset seiret RIA, täpsemalt Eesti rahvuslik CERT (*Computer Emergency Response Team*). Tegemist on RIA põhimääruse § 8 lg 4 punktist 4 tuleneva ülesandega. Seevastu aga süsteem, mida kasutaja otsustab pidada pilvsüsteemina teenusepakkuja tehnilisele lahendusele tuginedes, asendab varasema süsteemi, mille turvalisust sai RIA seirata. Sätte eesmärk on hoida ning edendada RIA seirevõimekusele tuginemisest tulenevaid eeliseid kasutajate süsteemide turvalisuse tagamisel.

Lõige 1 kehtestab kohustuse RIA-le pilvandmetöötlusteenuse kasutamisega kaasnevatele logide edastamiseks või muul moel kättesaadavaks tegemiseks.

Edastamine või muul moel juurdepääsu tagamine logidele peab võimaldama RIA-le analüüsida turvalisust ohustavaid riske. Selle nõude täitmiseks peab logide edastamine kasutajalt RIA-le koheselt pärast seda, kui logid on saabunud teenusepakkujalt kasutajale. Nõude täitmiseks on seega kasutajal mõistlik luua lahendus, kus logide edastamine toimub reaalajas ja automatiseeritult.

Kohustuslik on edastada pilvandmetöötlusteenuse kasutamisega kaasnevaid logisid ehk kasutaja ei pea ise arendama pilvsüsteemi toimingute logimissüsteemi, vaid edastama RIA-le seda, mida teenusepakkuja kasutajale edastab. Sisuliselt kohaldub nõue ennekõike pilvandmetöötlusteenuse kasutuslogidele. Samas logide sisu või vorminõue ei ole määratletud. Põhjuseks on logide mitmekesisus nii selle vormi kui ka sisu jaotustelt. Tuvastamaks, missuguseid logisid peaks kasutaja RIA-le edastama, on vaja vaadelda logide eesmärki. Kui logid võimaldavad analüüsida pilvsüsteemi turvalisust ohustavaid riske (näiteks päringulogid), siis on ka kohustus need logid edastada.

Kui pilvandmetöötlusteenuse pakkuja ei võimalda kasutajale teenuse osana juurdepääsu ühelegi kirjeldatud logile, siis puudub kasutajal ka kohustus logide edastamiseks. Kasutaja peaks eelistama siiski pilvandmetöötlusteenuse pakkujaid, kes võimaldavad kasutajatel ka seirata pilvsüsteemis tehtavaid toiminguid; lõikes kaks sätestatud juhtudel on sellise tingimuse täitmine ka pilvandmetöötlusteenuse kasutamise eeldus. Kui turvalisuse seireks vajalik logi sisaldab isikuandmeid, siis on nende RIA-le edastamise aluseks seadusliku kohustuse täitmine käesoleva sätte alusel. RIA poolt nende andmete töötlemine (seire) toimub samuti seadusliku

kohustuse täitmiseks vajaliku andmetöötluse alusel RIA põhimääruse alusel. Kui logi on määratud AK teabeks, siis on RIA ametniku juurdepääsu aluseks AvTS § 38 lg 3.

Lõige 2 kehtestab kohustuse kasutada vaid sellist pilvandmetöötlusteenuse pakkuja lahendust, mille kasutamisega kaasnevatele esimeses lõikes määratletud logidele võimaldab pakkuja juurdepääsu. Kohustus rakendub lõikes määratletud pilvsüsteemide pidamisele. Tegemist on pilvsüsteemidega, mille turvalisuse tagamiseks teostatava seire vajadus on kõrgendatud kas selles töödeldavate andmete konfidentsiaalsuse või süsteemide turvalisuse tagamise olulisusest tulenevalt. Esimeses punktis kirjeldatud pilvsüsteem on selgitatud laiemalt §-s 17 ning teises punktis kirjeldatud süsteem §-s 19.

Eelnõu § 19 kehtestab nõuded olulisema kaitsetarbega pilvsüsteemide käideldavuse tagamiseks. Kasutaja võib otsustada väga erinevate pilvsüsteemide pidamise kasuks, sealhulgas ka tema ülesannete täitmiseks vajalike süsteemide majutamiseks pilvsüsteemina. Sellistel juhtudel tuleb aga arvestada, et kasutaja kui organisatsiooni ülesannete täitmist mõjutava pilvsüsteemi käideldavus ei ole tehniliselt kasutaja poolt tagatav, vaid jääb sõltuma teenusepakkuja infrastruktuurist. Kui kasutaja samas ei peaks sellist süsteemi pilvsüsteemina (ehk *ei viiks sellist süsteemi pilve*), saaks toimepidevusriske maandada E-ITS-ile vastavad turvameetmete nõuded. Samuti on viimatised küberintsidendid selgelt näidanud, et isegi levinumate või suurimate teenusepakkujate pilvandmetöötlusteenuste käideldavus võib äkitselt kaduda.[31] Käesoleva paragrahvi eesmärk on seega tagada kasutaja ülesannete täitmiseks vajalike pilvsüsteemide käideldavus sõltumata pilvandmetöötlusteenuse käideldavusest.

Lõige 1 sätestab käesolev paragrahv kasutajale kohustuse suure käideldavusest tuleneva kaitsetarbega süsteemide pidamisel pilvsüsteemina pidada ka alternatiivset süsteemi või meedet.

Kasutaja peab seega alternatiivi pidamise nõuet täitma selliste süsteemide pilvsüsteemina pidamisel (nn *pilve viimisel*), mille kaitsetarvet on kasutaja hinnanud E-ITS-i järgi vähemal suureks (S) käideldavuse põhikomponendist tulenevalt. E-ITS-i järgimise kohustus on igal kasutajal ning selle järgimise käigus peab kasutaja ka kaardistama oma protsesside infovarad ja määrama neile kaitsetarbe. Kaitsetarve määratakse üldkorras kolme põhikomponendi järgi: konfidentsiaalsus, terviklus ning käideldavus. Sisuliselt antakse igale komponendile väärtus kasvaval skaalal: normaalne (N), suur (S) või väga suur (VS). Komponendi konkreetne väärtus sõltub selle komponendi häiritusest või kadumisest tuleneva kahjuliku mõju ulatusest kasutaja tegevusele. Seega tähendab süsteemi kaitsetarve S või VS käideldavuse suhtes seda, et kasutaja on hinnanud nimetatud süsteemi käideldavuse häirituse või isegi kadumise suureks või väga suureks kahjulikuks mõjuks oma tegevustele. Kui kasutaja otsustab seejärel pidada selliselt hinnatut süsteemi pilvsüsteemina, peab kasutaja pidama ka alternatiivset süsteemi või meedet.

E-ITS-le viitav määratlus kohustuse aluseks oleva süsteemi tuvastamisel on sätestatud eesmärgiga võimaldada kasutajal tugineda kohustuse täitmiseks juba tehtud tegevustele ning

[31] Näiteks on 2019. a blogipostituses https://davidmytton.blog/what-are-the-common-causes-of-cloud-outages/ toodud mõningad näiteid kolme suurima pilveandmetöötlusteenuse osutaja kohta; samuti on leheküljelt https://status.cloud.google.com/summary näha statistikat Google Cloud staatuse kohta, sisaldades ka ülevaateid intsidentide kohta.

vältida seega täiendava kaardistuse loomise ning haldamise kohustust. Samal eesmärgil on sätestatud ka kommenteeritava paragrahvi **lõikes 4**, et kui kasutaja rakendab rahvusvahelist standardit ISO/IEC 27001 E-ITS-i järgimise asemel, siis loetakse lõikes 1 sätestatud kohustuse aluseks selline süsteem, mis vastab kirjeldusele ISO/IEC 27001 kontekstis ehk samaväärsele riskitasemele. Kuivõrd ISO/IEC 27001 ei kehtesta nõuet (vaid soovitusi) süsteemi riskitaseme määratletud väärtusega hindamiseks, jääb ISO/IEC 27001 rakendamisel kasutaja kohustuseks määratleda *pilve viidavaid* süsteeme ka E-ITS-i kaitsetarbe perspektiivist, kui seda pole ISO/IEC 27001 kontekstis tehtud.

Peetav alternatiivne süsteem või meede peab vastama esimese lõike teises lauses sätestatud kriteeriumile. Puuduvad konkreetsed tehnilised nõuded või täieliku samaväärsuse nõue alternatiivi valimisel ja pidamisel. Tegemist peab olema alternatiiviga, mida kasutajal oleks võimalik ka pilvsüsteemi rikke korral rakendada, et kasutaja tegevus ja ülesannete täitmine saaks jätkuda. Samas ei pea alternatiiv olema aktiivselt kasutuses, kasutajal peab olema võimekus alternatiivi kasutusele võtta nii, et see ei sõltuks kolmandate osapoolte tahtest. Nõude täitmine ei eelda, et kasutaja peab pilvsüsteemi rikke korral olema võimeline täitma sellest sõltuvaid ülesandeid täies mahus. See, et alternatiiv võib olla väiksema võimekusega, saab olla kasutaja poolt vastuvõetav risk, kui selline risk on kaardistatud ja selgelt vastu võetud. Peamiseks nõude täitmise hindamise aluseks on, et kasutaja suudab oma ülesandeid ka pilvsüsteemi rikke korral täitma jääda.

Lõige 2 kehtestab nõuded peetavale alternatiivile kasutatava pilvandmetöötlusteenuse pakkujaga seonduvalt. Lõikes sätestatud kriteerium on sisuliselt tehnoloogilise sõltumatuse nõue. Pilvsüsteemi käideldavusega seonduv risk ei oleks maandatud, kui kasutaja soetaks näiteks sama teenust kaks korda, sest sellisel juhul ei töötaks intsidendi korral kumbki lahendus. Ei ole küll tehniliselt võimalik ega ka eeldatav, et alternatiiv oleks töökorras kogu aeg, kuid kasutataval lahendusel ja alternatiivil ei tohiks olla tehnoloogilisi ristsõltuvusi (süsteemi pidamisega seonduvalt, mitte elektri- või internetiühendusest tulenevalt). Samas ei ole välistatud, et nii pilvsüsteem kui ka alternatiiv tuginevad mõlemad pilvandmetöötlusteenusele või sama pakkuja erinevatele teenustele. Sellistes olukordades peab aga kasutaja suutma tõendada, et nii pilvsüsteem kui ka peetav alternatiiv on tehnoloogiliselt sõltumatud lahendused.

Lõige 3 kehtestab nõuded alternatiivi pidamisele pilvsüsteemi suhtes toimunud terviklust või käideldavust mõjutava küberintsidendi korral. Käideldavust mõjutav küberintsident ei pruugi tähendada, et pilvsüsteemi käideldavus täielikult puudub, ka osaline käideldavuse häiritus või sündmus, mis ohustab käideldavust, on käsitletav küberintsidendina KüTS § 2 punkti 3 tähenduses. Küberintsidendi toimumisel peab kasutaja tegema seega kõik vajalikud toimingud, et kasutajal oleks võimalik alustada pilvsüsteemi asemel alternatiivi rakendamist viivitamatult. Koheselt peab kasutaja hakkama alternatiivi rakendama siis, kui see on vajalik oma tegevuste jätkamiseks, näiteks kui käideldavus on juba küberintsidendi alguses täielikult kadunud või on selleks suur oht. Alternatiivi tuleb kasutada ka juhul, kui on aset leidnud kasutatava lahenduse terviklust mõjutav küberintsident.

Eelnõu §-id 20, 21 ja 22 (4. peatükk) on rakendussätted.

Eelnõu § 20 sisustab lühiajalise erandi E-ITS-le üleminekuks.

Paragrahv kehtestab KüTS-i subjektidele võimaluse täita E-ITS-i rakendamise asemel seni subjektidele kehtinud küberturvalisuse turvameetmete nõudeid. Tegemist on E-ITS-i rakendamise edasilükkamist võimaldavate lõigetega, mille kehtivus on ajaliselt piiratud 2022. aasta lõpuni. Sarnaselt eelnõu § 3 lõikega 2, käsitletakse siinsetes lõigetes sätestatud nõuete täitmise korral E-ITS-i järgimise ja selle järgimisest tulenevate turvameetmete rakendamise kohustus täidetuks.

Lõige 1 sätestab E-ITS-i rakendamise edasilükkamise võimalused avalikule sektorile. Sätte sõnastus on üle võetud kehtetuks tunnistatava KüTS § 9 lõikest 2. Kuigi ISKE turvameetmete nõuetele viitav norm tunnistatakse 531 SE-ga kehtetuks, on ISKE volitusnorm AvTS--is kehtiv sarnaselt käesoleva sättega 2022. aasta lõpuni.

Lõige 2 sätestab E-ITS-i rakendamise edasilükkamise võimalused muudele KüTS-subjektidele, ennekõike KüTS § 3 lõikes 1 loetletud teenuse osutajatele. Sisuliselt on sätte eesmärgiks võimaldada E-ITS-i rakendamise edasilükkamist, kui subjekt täidab kehtetuks tunnistatava KüTS § 7 lõike 4 alusel sätestatud nõudeid. Kuivõrd nõuded on tunnistatakse 531 SE-ga kehtetuks, ei saa neile ka käesolev määrus viidata, vaid on vajalik nimetatud nõuete sisuline ülevõtmine sättesse kuni üleminekuperioodi lõpuni. Käesoleva lõikega on üle võetud kehtetuks tunnistatava KüTS § 7 lõike 4 alusel kehtestatud turvameetmete nõuded. Kehtetuks tunnistatava KüTS § 7 lõike 4 alusel kehtestatud määruses sätestatakse ka nõuded süsteemide suhtes läbiviidavatele riskianalüüsidele, kuid käesolev lõige neid nõudeid üle ei võta. Viidatud riskianalüüsinõuded ei vaja oma üldisuse tasemest tulenevalt käesolevasse määrusesse ülevõtmist, kuivõrd põhjustaksid eelnõu §-des 5 ja 6 sätestatud nõuete dubleerimist. Kuivõrd §-des 5 ja 6 sätestatud nõuded on eraldiseisvad E-ITS-i järgimise kohustusest (küll võimaldab E-ITS-i järgimine riskianalüüsi nõuded eraldiseisva tegevuseta täita eelnõu § 5 lõike 2 alusel), ei ole riskianalüüsi nõuete eraldi sätestamine käesolevas lõikes vajalik ka riskianalüüsi läbiviimise kohustuse olemasoluks.

Eelnõu § 21 kehtestab tähtajad E-ITS-i järgimise esmakordsele auditeerimisele. E-ITS-i järgimise auditeerimiskohustus tuleneb E-ITS-ist endast ning eelnõu § 4 lõikest 1. Üldreegel on, et audit tuleb läbi viia iga kolme aasta järel.

Esmakordse auditeerimise läbiviimiseks sätestatakse aga erikord, sest ISKE auditeerimistähtajad varieeruvad 2-4 aasta vahel ning seda asendav E-ITS kasutab ühtset kolmeaastast intervalli. Samuti on ka vaja õigusselgust nende teenuse osutajate osas, kes ei pea ISKE-t rakendama.

Seega on iga auditeerimiskohuslase esmakordse auditi läbiviimise tähtajaks ISKE auditi aegumine, kui see aegub enne kolme aasta möödumist käesoleva määruse jõustumisest. Teenuse osutajad, kes ISKE-t ei rakenda või kelle ISKE audit aegub hiljem, peavad esmakordse auditeerimise läbi viima kolme aasta jooksul.

Esmakordse auditi läbiviimise tähtaja eriregulatsioon võimaldab ISKE-t järgival teenuse osutajal lükata edasi tähtaja saabumist täiendava ISKE auditi läbiviimise kaudu enne 2023. aasta 1. jaanuarit (alates millest ISKE järgimise kohustus muutub kehtetuks).

Organisatsioon, kes muutub teenuse osutajaks pärast käesoleva määruse jõustumist, viib esmakordse auditi läbi kolme aasta jooksul alates teenuse osutajaks muutumisest, mitte ei pea subjekt lähtuma käesoleva määruse jõustumiskuupäevast.

Eelnõu § 22 sätestab määruse jõustumise.

Määrus jõustub 531 SE-ga samal ajal, kuid mõne olulise erandiga.

Määruse §-id 7 kuni 11 jõustuvad 1. jaanuaril 2023. aastal. Tegemist on andmekogude erisustest tulenevate nõuetega E-ITS-i järgimisel, mis tulenevad ennekõike ISKE nõuetest. Erisused jõustuvad seega ka hetkest, kui ISKE nõuded kehtetuks muutuvad. Need muudatused toimuvad 531 SE tõttu AvTS-i muudatustega.

Määruse §-id 14 kuni 19 jõustuvad 1. jaanuaril 2024. aastal. Tegemist on pilvsüsteemide pidamisega seonduvate nõuetega. Nõuetega vastavusse jõudmiseks juba olemasolevate pilvsüsteemide pidamisel on seega kasutajatele sätestatud üleminekuaeg 2024. aasta 1. jaanuarini.

Eelnõu koostajad märgivad, et E-ITS-i järgimise kohustuse jõustumine üldises korras ei tähenda nõuet, et E-ITS-i järgija peab olema jõudnud selle kohustuse ehk 531 SE ning siinse eelnõu jõustumise hetkeks juba rakendada kõik järgimisest tulenevad turvameetmed. Selline olukord ei ole ka võimalik, sest E-ITS-i järgimine on tsükliline protsess; isegi konkreetse turvameetme rakendamine ei tähenda, et E-ITS-i järgimise protsess oleks kuidagi „lõpule viidud“. E-ITS-i järgimise kohustuse täitmine on hinnatav läbi teenuse osutaja tegevuste või tegevusetuse hindamise infoturbe korraldamisel ning esimene arvestatav ülevaade kohustuste järgimisest tekib pärast esmakordse auditi läbiviimist.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei oma puutumust Euroopa Liidu õigusega.

4. Määruse terminoloogia

Eelnõu terminid tuginevad KüTS-s ning AvTS-s sisustatud terminitele. Määruses kasutatakse samuti Eesti infoturbestandardis määratletud termineid ning täiendavalt luuakse määrusega terminid „infoturve“ ja „pilvandmetöötlusteenusel põhinev süsteem“ ehk „pilvsüsteem“. Andmekogudega seonduvalt määratletakse ka andmete käideldavuse, tervikluse ja konfidentsiaalsuse sisu – need kehtivad ainult §-de 7-11 olukorras.

1) Andmekogu on andmekogu avaliku teabe seaduse § 43^1 lõike 1 tähenduses.

2) Infoturve on võrgu- ja infosüsteemile turvameetmete loomise, valimise ja rakendamise protsesside kogum.

3) Pilvsüsteem on süsteem või süsteemi osa, mille pidamist teostab teenuse osutaja pilvandmetöötlusteenust kasutades.

4) Andmete käideldavus on eelnevalt kokku lepitud vajalikul ja nõutaval tööajal kasutamiskõlblike andmete õigeaegne ning hõlbus kättesaadavus (st vajalikul ja nõutaval ajahetkel ning vajaliku ning nõutava aja jooksul) selleks volitatud isikule või tehnilisele vahendile.

5) Andmete terviklus on andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.

6) Andmete konfidentsiaalsus on andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile.

5. Määruse mõjud

Määruse eelnõu mõjude hindamine on selguse huvides läbi viidud muutuste kategooriate suhtes eraldi. Analüüsitavateks muudatusteks on:

1) E-ITS-i kehtestamise volitamine;

2) avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded;

3) pilvsüsteemi pidamise nõuded.

Määruse eelnõu 3. peatüki 1. jao ning 2. jao 1. jaotisel hinnatav oluline mõju puudub.

3. peatüki 1. jagu (eelnõu §-id 5 ja 6) kehtestab teenuste kaardistuse ja turvameetmete dokumentatsiooni nõude, mis täpsustab samasisulisi nõudeid KüTS § 7 lg 2 punktide 1, 2 ja 6 alusel. Dokumentatsiooni säilitamise tähtaja pikendamine kolmelt aastalt seitsmele aastale võimaldab teostada dokumentatsiooni ajakohasuse järelevalvet kahe auditeerimistsükli ulatuses ning ei kujuta kohuslastele hinnatavat olulist mõju.

3. peatüki 2. jao 1. jaotise eesmärk andmekogude pidamise erisuste kehtestamisel on võimaldada üleminek ISKE asendamisel E-ITS-ga andmekogude suhtes säilitades olemasolevad nõuded, mistõttu sätetel iseseisvat mõju E-ITS-i kehtestamise mõjudest eraldiseisvalt ei ole.

5.1. Kavandatav muudatus: E-ITS-i kehtestamise volitamine

E-ITS-i kehtestamisega seotud mõjud on ulatuslikult analüüsitud küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse eelnõu 531 SE[32] seletuskirjas (seletuskirja punkt 6.1. ning selle alapunktid; lk-d 33-39), kuivõrd nimetatud eelnõu sätestas volitusnormi käesoleva kavandatava määruse kehtestamiseks. Järgnev analüüs on seega suuresti eelnimetatud eelnõu mõjude analüüsi vastava peatüki kordus.

[32] Küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seadus 531 SE – kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/K%C3%BCberturvalisuse%20seaduse,%20avaliku%20teabe%20seaduse%20ja%20Eesti%20Rahvusringh%C3%A4%C3%A4lingu%20seaduse%20muutmise%20seadus.

5.1.1. Sotsiaalne, sh demograafiline mõju

5.1.1.1. Mõju ettevõtjale

Eelnõu ei tekita ettevõtjale sotsiaalset mõju. Teenuse osutajate vajadus tööturul sobiva kvalifikatsiooniga küberturbe ekspertide järele küberturvalisuse tagamiseks jääb püsima.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.1.2. Mõju kodanikele

Eelnõu tekitab kodanikele positiivset sotsiaalset mõju. Vene Föderatsiooni sõjaline (sh kübertasandil) agressioon iseseisva demokraatliku riigi vastu viitab ohule ka võimalike küberrünnakute korraldamiseks Eesti teenuse osutajate vastu. Praktikas toimub igapäevaselt Eesti küberruumi vastu suunatud tegevusi, mida tõendavad RIA koostatavad ülevaated.[33] Eesmärk E-ITS-i kehtestamise kaudu tugevdada küberturvalisuse taset parandab avalike ja elutähtsate teenuste toimepidevust, seega kuigi Eestis ei ole käesoleva eelnõu koostamise hetkel elutähtsate või avalike teenuste toimepidevus ohustatud, aitab eelnõu positiivselt kaasa selle seisukorra säilitamisele.

Ulatus keskmine, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.2. Mõju riigi julgeolekule ja välissuhetele

5.1.2.1. Mõju ettevõtjatele

KüTS-i mõistes teenuse osutajad pakuvad ühiskonna toimimiseks vajalikke teenuseid. E-ITS-i kehtestamise eesmärk on täpsustatud ja selgema infoturbe haldamissüsteemi rakendamisega aidata edendada teenuse osutaja ning tema teenuste vastupanuvõimet küberintsidentidele, ning sellest tulenevalt on eelnõul positiivne mõju riigi julgeolekule.

Eelnõu ei mõjuta otseselt ettevõtjate välissuhteid, kuivõrd teenuse osutajatel on ka edaspidi võimalik E-ITS-i rakendamise asemel rakendada küberturvalisuse tagamisel ka rahvusvahelist ISO/IEC 27001 standardit. Kaudselt on eelnõul positiivne mõju välissuhete edendamisele tugevama küberturvalisuse kuvandi tõttu.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

5.1.2.2. Mõju avalikule sektorile

Eelnõul on positiivne mõju riigi julgeolekule ka avaliku sektori kaudu. Selgema avaliku sektori määratluse 531 SE tulemusel ning E-ITS-i kehtestamisega kehtiva ISKE asemel on avalikus sektoris ka suurem selgus, et kes ja mida tegema peab. Samuti vähendab E-ITS-i organisatsioonipõhine lähenemine küberturvalisuse tagamisel ka avaliku sektori haavatavust küberintsidentidele ning nende mõjude levimist avalike sektori jaoks olulisemate süsteemideni.

Välissuhete vaatepunktist aitab avaliku sektori küberturvalisuse nõuete uuendamine ka säilitada ning arendada Eesti riigi kui küberturvalisuse eestvedaja kuvandit.

[33] Kättesaadavad siit: https://www.ria.ee/et/kuberturvalisus/olukord-kuberruumis.html.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

5.1.2.3. Mõju järelvalveasutusele (RIA-le; julgeolekuasutustele)

Eelnõu aitab RIA-l läbi täpsemate küberturvalisuse tagamise nõuete tugineda küberintsidentide ennetamisel, tuvastamisel ja lahendamisel ühtsematele eeldustele teenuse osutajate ja avaliku sektori turvameetmete suhtes. Samuti aitab eelnõu läbi reguleeritud auditeerimistingimuste tagada selgema ja kiiremini analüüsitava ülevaate küberturbe tasemest Eestis. Sellest tulenevalt on eelnõul positiivne mõju RIA riigikaitse ja julgeolekuga seotud valmisolekule küberintsidentide ennetamiseks, tõrjumiseks ja lahendamiseks.

531 SE-ga tehakse ka erisus julgeolekuasutustega seotud süsteemide järelevalve osas. Julgeolekuasutuste puhul puuduvad olulised mõjud riigi julgeoleku ja välissuhete osas. Julgeolekuasutustele (enda süsteemide üle järelevalve teostamisel) avalduvad sarnased mõjud, mis RIA-le (vt eelmist tekstilõiku).

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

5.1.3. Mõju majandusele

5.1.3.1. Mõju ettevõtjatele

E-ITS-i kehtestamisest tulenevad muutused kujundavad formaalselt ümber teenuse osutajate kohustusi, kuid ei muuda neid sisuliselt võrreldes varasemate kohustustega küberturvalisuse tagamisel. Kehtiva KüTS § 7 lõike 1 alusel peavad teenuse osutajad juba praegu rakendama turvameetmeid ning kehtinud lõike 2 alusel koostama süsteemide riskianalüüse. Neid kohustusi sisustab KüTS § 7 lõike 4 alusel kehtestatud määrus (viidatud määruse volitusnorm tunnistatakse 531 SE-ga kehtetuks).

Muudatusega ei lähtuks teenuse osutajad nõuete täitmisel KüTS § 7 lõike 4 alusel kehtestatud määrusest, vaid käesolevast eelnõust. E-ITS on kindlasti mahukam dokument kui KüTS § 7 lõike 4 alusel kehtestatud määrus, kuid selle põhjuseks on nõuete põhjalikum kirjeldus, mitte nõuete oluline laiendamine. Sarnaselt veel kehtiva KüTS § 7 lõike 4 alusel kehtestatud määruses sisustatud nõuetega, põhinevad ka E-ITS-i nõuded organisatsiooni riskianalüüsile ja selle põhjal rakendatud turvameetmetele. Seega eeldusel, et teenuse osutaja on varasemalt teinud pingutusi küberturvalisuse tagamiseks KüTS § 7 lõike 4 alusel kehtestatud määruse nõuete järgimisega, ei tulene teenuse osutajale E-ITS-i tingimuste järgimise kohustusest suurt majanduslikku mõju. Lisaks säilitab eelnõu kuni 31. detsembrini 2022. a KüTs § 7 lõike 4 alusel antud määruse põhilised nõuded – vt eelnõu § 20, sh nende kahe lõike selgitusi.

E-ITS-i kehtestamisega kaasneks ettevõtjatele kohustus läbi viia E-ITS-i vastavusaudit iga kolme aasta järel. Eelnõuga asendatakse KüTS § 7 lõike 2 punktide 5 ja 6 alusel kehtinud kohustus viia läbi ning dokumenteerida turvameetmete rakendamise piisavuse kontroll. Kehtinud nõuete kohaselt oli turvameetmete rakendamise piisavuse kontrolli üks meetoditest auditi läbiviimine pädeva sõltumatu isiku poolt, mida võis asendada ka nn enesehindamisega. E-ITS-i kehtestamise järgselt kaoks võimalus asendada audit enesekontrolliga ning E-ITS sätestab konkreetse raamistiku auditite läbiviimiseks eesmärgiga tagada selgem ja läbipaistvam küberturvalisuse nõuete järgimine. Teenuse osutajatele, kes varasemalt teostasid

turvameetmete rakendamise piisavuse kontrolli nn enesehindamise kaudu, võib muudatus avaldada majanduslikku mõju, kuid seda maksimaalselt ulatuses, mis oleks nn enesehindamise läbiviimise ja auditi läbiviimise kulude vahe. Ei ole otseselt hinnatav, kas E-ITS-i vastavusaudit on ettevõtjale soodsam või kulukam kehtinud KüTS § 7 lõike 2 punkti 5 alusel läbiviidud kontrollidest. Kui ettevõtjal on vastavushindamise läbiviimiseks endal sobivad spetsialistid, siis võib tekkiv E-ITS-i auditite läbiviimise kohustus olla kulukam kui seni KüTS § 7 lõike 2 punkti 5 alusel läbiviidud kontroll, mis oleks nn enesehindamisega läbi viidud. Siinkohal saab ettevõtja täiendavaid kulusid minimeerida põhjaliku eeltööga E-ITS-i auditi tellimiseks ja läbiviimiseks. Kui ettevõtja on aga kehtinud KüTS § 7 lõike 2 punktis 5 sätestatud kohustuste täitmiseks tellinud vastavushindamisi teenusepakkujatelt, siis võib tekkiv E-ITS-i auditite läbiviimise kohustus olla soodsa majandusliku mõjuga. Soodne majanduslik mõju võib tuleneda asjaoludest, et E-ITS-i audit oleks rohkem standardiseeritud teenus, mis tugineb ka põhjalikuma täpsusastmega standardiseeritud nõuete kogumi vastavuse hindamisel. Kuivõrd E-ITS-i läbiviimise audit ei ole veel turul pakutav teenus, siis ei ole võimalik hindade täpset võrdlust käsitleda. Samas on olemas teenuse osutajaid, kes auditeerimisteenust pakuvad.[34]

On võimalik, et auditeerimiskulud on majanduslikult koormavamad subjektidele, kelle IKT korraldus on oluliselt väiksema mahuga, kuivõrd ühine lävend ja seega ka minimaalne kulu auditi teenuse läbiviimises tuleneb protseduurist auditi läbiviimisel, kvalifikatsiooninõuetest auditi läbiviijale ning auditi käigus koostatava dokumentatsiooni nõuetest. Seega on majandusliku mõju tasakaalustamiseks käesoleva määruse § 4 lg 3 punktis 1 ettenähtud ka erand mikroettevõtjatele (nt suurele osa tegutsevatele perearstidele). Erand on kavandatud konkreetselt auditite läbiviimise kohustuse suhtes, mitte E-ITS-i järgimise kohustuse suhtes.

Täiendavalt toetab RIA ka E-ITS-le üleminekut ettevõtjatele koolituste läbiviimisega E-ITS-i rakendamiseks. Arvestamaks samaliigiliste ettevõtjate sarnast profiili IKT korraldamisel on RIA-l ka kavas võimaluste piires E-ITS-i rakendamise profiilide loomine, mis võimaldab konkreetset tüüpi ettevõtjatel (nt perearstidel ja teistel teenuse osutajatel) veel lihtsustatumas korras RIA poolt pakutavate lahenduste ja kavandatavate meetmete toel E-ITS-i rakendada.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.3.2. Mõju avalikule sektorile

E-ITS kehtestamisega asendatakse AvTS-i alusel kehtinud ISKE järgimiskohustus. Eeldusel, et avaliku sektori rakendaja on järginud ISKE nõudeid, puudub ISKE ja E-ITS-i nõuete võrdluses E-ITS-i kehtestamisest tulenev majanduslik mõju avalikule sektorile nii turvameetmete rakendamisel kui ka vastavusauditite läbiviimisel. Majanduslik mõju avalikule sektorile, mis tuleneb täpsemalt raamistatud organisatsioonipõhisest lähenemisest küberturvalisuse tagamisel (sh kaardistustegevused ja riskianalüüsid) on minimaalne ning praktikas rakendatav läbi E-ITS-i üleminekujuhendite kasutamise.[35] Üleminekuperioodil võib arvestada ajutiselt suurenenud ressursi vajadusega, et tutvuda uue standardiga. Samas on RIA üleminekut toetamas juba alates 2020 aasta algusest: a) kaasates kõiki avaliku sektori infoturbejuhte E-ITS-i väljatöötamisse; b)

[34] Vt https://www.eisay.ee/iske-e-its-ja-iso-27001-alaste-teenustega-tegelevate-ettevotete-loetelu.
[35] Üleminekujuhend on kättesaadav siit: https://eits.ria.ee/et/versioon/2020vers1/juhendid/ueleminekujuhend-iskelt-eitsile/.

korraldades koolitusi[36], mis tutvustavad E-ITS-i sisu ja selle rakendamist; c) viies läbi pilootprojekti E-ITS-i rakendamiseks; d) koostades muuhulgas üleminekujuhendi. Kõik need toetavad tegevused jätkuvad.

E-ITS-i kehtestamisega on mõju avalikule sektorile vaadeldav kolme stsenaariumi alusel lähtuvalt subjektile varasemalt kehtinud nõuetest:

1) Stsenaarium 1: E-ITS asendab ISKE järgimise kohustuse kõikide süsteemide suhtes (suurem osa kohaldamisalast).

E-ITS-i ülevõtmiseks rakendatakse selleks otstarbeks koostatud üleminekujuhendit. ISKE nõuetekohase rakendamise korral E-ITS-i ülevõtmisega RIA hinnangul täiendavaid rahalisi kulusid üldjuhul ei kaasne, aga kaasneb ajakulu senise dokumentatsiooni vastavusse viimiseks. E-ITS-i juurutamise etapis tuleb arvestada, et infoturbe rolli täitvatel inimestel kulub põhitöö kõrvalt täiendavalt aega E-ITS-i nõuete ülevõtmiseks.

Kui subjektil on olnud ISKE järgimise kohustus kõikide süsteemide suhtes, kuid see ei ole nõuetekohaselt täidetud, siis selle subjekti süsteemi turvalisuse tagamiseks vajalikud kulutused E-ITS-iga vastavusse jõudmisel ei kuulu eelnõu majandusliku mõju analüüsi alla. Eelnõu koostamine lähtub eeldusest, et kehtivaid seaduslikke nõuded täidetakse ning käsitleb eelnõuga kehtestatavate nõuete mõju vastu varasemate nõuete mõju. Avalik sektor peab oma eelarve planeerimisel seisma selle eest, et IT-lahenduste arendamine ning kasutuselevõtt toimuks vaid nende süsteemide küberturvalisuse tagamiseks vajalike ressursside olemasolul.

2) Stsenaarium 2: E-ITS-i ülevõtmise kohustusele ei eelnenud varasemalt küberturvalisuse tagamise nõudeid (nt osad avalik-õiguslikud juriidilised isikud).

Sarnaselt esimese stsenaariumiga tuleb arvestada infoturbe rolli täitvate inimeste ajakuluga E-ITS-i ülevõtmiseks vajalike dokumentatsioonide koostamisel. Ajakulu on suurem selles osas, milles dokumentatsioon, sh vajalikud kaardistused, kuuluks esmakordselt koostamisele.

Erinevalt esimesest stsenaariumist kaasneb üldjuhul ka rahaline kulu süsteemide turvalisust tagavate meetmete rakendamisel. Majanduslik mõju selles stsenaariumis on igale subjektile väga erinev ning ei oleks analüüsis mõistlikult hinnatav. Turvameetmete rakendamiseks vajalik rahaline kulu sõltub subjekti kasutatavate süsteemide hulgast, keerukusest ning nendele ka eelnevalt rakendatud turvameetmete olemasolust (tulenevalt subjekti vastutustundlikkusest oma IT-lahenduste kasutamisel või muudest seaduslikest nõuetest, näiteks isikuandmete töötlemiseks rakendatud tehnilisi ja korralduslikke meetmeid turvalisuse tagamiseks). Rakendamiseks vajaliku kulu majanduslik mõju subjektile sõltub omakorda selle kulu osakaalust subjekti eelarves, ennekõike IT-lahendustega seotud eelarves.

[36] Vt https://eits.ria.ee/et/avalehe-menueue/koolitus/ ning https://www.ria.ee/et/kalender.html.

Selle stsenaariumi korral võib mõnele subjektile tekkida eelnõust tulenevalt oluline majanduslik mõju, kui subjekt kasutab oma tegevuses ulatuslikult keerukaid süsteeme, millele turvameetmeid varasemalt rakendatud ei ole ning mille eelarve ei ole lihtsasti võimeline nende IT-lahenduste toimepidevuse tagamiseks vajalikke ressursse teenindama. Küll aga ei mõjuta see olukord majandusliku mõju hinnangut avalikule sektorile tervikuna, kuivõrd tegemist oleks ühe osaga väga piiratud subjektide ringist.

3) Stsenaarium 3: E-ITS asendab ISKE järgimise kohustuse, ning laiendab nõuete kohaldamisala andmekogudelt kõikidele süsteemidele (andmekogude vastutavad või volitatud töötlejad, kes ei olnud KüTS-i subjektid, sh mitmed avalik-õiguslikud juriidilised isikud).

Sarnaselt eelnevatele stsenaariumitele kaasneb ka selle stsenaariumi puhul E-ITS-ist järgimisest tulenev ajakulu infoturbe rolli täitvatel inimestel.

Sarnaselt teise stsenaariumiga kaasneb üldjuhul ka rahaline kulu süsteemide turvalisust tagavate meetmete rakendamiseks, mille ulatus ning ulatusest tulenev majanduslik mõju on igale subjektile erinev.

Stsenaariumis on aga vajalik ajaline kui ka rahaline kulu oluliselt piiratum teisest stsenaariumist, kuivõrd subjekt on järginud ISKE nõudeid andmekogude turvalisuse tagamiseks. Samuti on ka käesoleva subjektide ring väga piiratud kehtinud KüTS § 9 lg 1 kohaldamisalaga võrreldes, ega mõjuta ka seega oluliselt eelnõust tulenevat majandusliku mõju hinnangut avalikule sektorile.

Täiendavalt on majandusliku mõju hindamiseks oluline märkida, et isegi kui eelnõust tulenevalt peab subjekt võtma rahalisi kohustusi süsteemide turvalisuse tagamiseks, siis võib nende kulude mõju olla subjektile majanduslikult positiivne. Süsteemide turvalisuse tagamiseks tehtavad kulutused vähendavad nii küberintsidendi tekkimise tõenäosust kui ka tekkinud küberintsidendi kahjulikku majanduslikku mõju. Arvestades küberruumis aina sagedamini esinevaid rünnakuid,[37] suuresti ka avaliku sektori süsteemide vastu, ning nende laastavat mõju ohvri süsteemide kasutatavusele, ei oleks õigustatud ka süsteemide turvalisuse tagamiseks tehtavaid kulutusi vaadelda rangelt kahjuliku majandusliku mõjuna.

Sarnaselt ettevõtja majandusliku mõju hinnanguga on ka võimalik, et auditeerimiskulud on majanduslikult koormavamad nendele avaliku sektori subjektidele, kelle IKT korraldus on oluliselt väiksema mahuga, kuivõrd ühine lävend ja seega ka minimaalne kulu auditi teenuse läbiviimises tuleneb protseduurist auditi läbiviimisel, kvalifikatsiooninõuetest auditi läbiviijale ning auditi käigus koostatava dokumentatsiooni nõuetest. Seega on majandusliku mõju tasakaalustamiseks käesoleva määruse § 4 lg 3 punktis 2 ettenähtud ka erand avaliku sektori subjektidele, kelle IKT korraldus on subjekti ülesannetest lähtuvalt piiratum (nt muuseumid, raamatukogud, etendusasutused). Erand on kavandatud konkreetselt auditite läbiviimise kohustuse suhtes, mitte E-ITS-i järgimise kohustuse suhtes.

[37] Vt nt RIA ööpäeva ülevaadet Eesti küberruumi kohta: https://www.ria.ee/et/kuberturvalisus/olukord-kuberruumis/oopaeva-ulevaated.html.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.3.3. Mõju kodanikele

E-ITS-i kehtestamise eesmärk on selgema raamistiku kaudu edendada süsteemide turvalisust. Sellel on vahetu mõju majanduskeskkonna toimimisele, kuivõrd Eesti konkurentsieelis digilahenduste kasutuselevõtus ja arendamises on tugevalt seotud nende digitaalsete lahenduste ja sealse andmetöötluse toimepidevuse, tervikluse ning konfidentsiaalsuse tagamisega. Samuti mõjutab eelnõu kodanikke digitaalseid teenuseid rohkem usaldama, tagades seega ka nende toimimise jätkusuutlikkuse suureneva kasutamise kaudu.

Kodanike halduskoormust eelnõu ei mõjuta.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.4. Mõju elu- ja looduskeskkonnale

Eelnõu ei avalda otsest mõju elu- ja looduskeskkonnale. Kaudselt võib eelnõu positiivset mõju elu- ja looduskeskkonnale aga avaldada läbi vastupanuvõimekuse suurendamise küberrünnakute suhtes, mis saaksid põhjustada elukeskkonnale või looduskeskkonnale kahjulikke tagajärgi (nt veepuhastusprotsessi sekkumine ja kasutatavate kemikaalide koguste muutmine).

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.5. Mõju regionaalarengule

Seaduseelnõu ei oma olulist mõju regionaalarengule.

5.1.6. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

5.1.6.1. Mõju avalikule sektorile

Eelnõu ei mõjuta avaliku sektori töökorraldust, kuivõrd ka varasemate nõuete alusel oli avalik sektor kohustatud kõikidele võrgu- ja infosüsteemide küberturvalisuse tagamisel järgima ISKE nõudeid. E-ITS-i kehtestamine ei too kaasa muudatusi, mille rakendamine vajaks asutuse töökorralduse või selles osas töökoormuse olulist suurendamist.

Eelnõu võib kaudselt mõjutada avaliku sektori teenuste kvaliteeti, kuivõrd teenuste kaardistamise ja riskipõhine lähenemine aitab asutusel tuvastada tehnoloogilisi mahajäämusi või paremaid arendussuundi. Ühtlasi aitab E-ITS-i rakendamise eelduseks olev selge ülevaade asutuse äriprotsessidest ja nendega seotud teenustest hinnata asutuse toimimiseks vajalike ressursside kasutamist. Siinse kaardistuse puhul on abiks protsesside kaardistus, mis on teostatud TKTA määruse alusel.[38] Sel teemal vaata ka eelnõu § 5 lõike 3 selgitusi.

Mõju avaliku sektori kuludele võib eelnõu kehtestamisel esineda vastavalt punktis 5.1.3.2 esitatud analüüsile neil juriidilistel isikutel ja asutustel, kes varasemalt ei ole olnud kõikide süsteemide osas ISKE kohuslased, ning ühtlasi pole teinud pingutusi kasutatavate võrgu- ja

[38] Vabariigi Valitsuse 25.05.2017 määrus nr 88 „Teenuste korraldamise ja teabehalduse alused“; RT I, 25.03.2021, 6.

infosüsteemide turvalisuse tagamiseks. Sellisel juhul suurendab E-ITS-i kehtestamine kulutuste tegemise vajadust pädeva personali palkamiseks, asjakohaste turvameetmete rakendamiseks ning auditite läbiviimiseks, samas vähendades kulutuste tegemise vajadust küberintsidentidest tuleneva kahju või muude tagajärgede likvideerimiseks.

Sellegipoolest oleks ka siis mõjude ulatus väike, kuivõrd kohustusi avalikule sektorile tehniliste ja korralduslike turvameetmete rakendamiseks tuleneb ka mujalt. Ennekõike peab sõltumata KüTS-is sätestatud kohustustest avalik sektor rakendama isikuandmete turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid isikuandmete kaitse üldmääruse artikkel 32 lõike 1 alusel ning samuti lähtuma selle kohustuse täitmisel riskide analüüsist isikuandmete kaitse üldmääruse artikkel 32 lõike 2 alusel.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.6.2. Mõju järelvalveasutusele (RIA-le; julgeolekuasutustele)

E-ITS-i kehtestamise eesmärgi raames ei mõjuta eelnõu RIA töökorraldust. Varasem KüTS § 7 lõike 4 alusel kehtestatud nõuete ja ISKE nõuete järgimise kontroll asendub E-ITS nõuete järgimise kontrolliga.

RIA töökoormust võib eelnõu suurendada suurema hulga auditite järeldusotsuste ülevaatamise vajaduse tõttu, kuid samuti ka vähendada tänu küberturbe korralduste kui ka auditite põhjalikumale standardiseeritusele.

531 SE-ga tehakse ka erisus julgeolekuasutustega seotud süsteemide järelevalve osas. Julgeolekuasutuste puhul on eeldatavasti teatavad mõjud, kuid kuna auditid on standardiseeritud, siis see mõju ei ole oluline.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.1.7. Muu otsene või kaudne mõju

Seaduseelnõu ei oma muud otsest või kaudset olulist mõju.

5.2. Kavandatav muudatus: avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded

5.2.1. Sotsiaalne, sealhulgas demograafiline mõju

Eelnõuga kaasneb positiivne sotsiaalne mõju. Eelnõu kehtestamisega tagatakse efektiivsemalt Eesti riigi kodanikele Eesti riigi järjepidevus ning edasi toimimine, luues aluse võimaldamaks teostada elutähtsate teenuste pakkumist ka siis, kui Eesti riigis paiknevad andmekeskused ei tööta, olgu selle taga siis looduskatastroof, elektrikatkestus või sõjaline rünnak.

Ulatus keskmine, sagedus väike, ebasoovitavate mõjude risk väike.

5.2.2. Mõju riigi julgeolekule ja välissuhetele

Eelnõuga kaasneb positiivne mõju riigi julgeolekule, lisades turvalisust Eesti omariiklusele ja digitaalsele järjepidevusele. Eelnõu kehtestamisega tagatakse riigi ja kohaliku omavalitsuse

funktsioonide ning elutähtsate teenuste pakkumiseks andmete säilitamine ja nende taaskasutamise võimalus. See tähendab, et Eesti riigi toimimine saab efektiivsemalt jätkuda ka siis, kui Eestis paiknevad andmekeskused ei tööta, olgu selle taga siis looduskatastroof, elektrikatkestus või sõjaline rünnak.

Ulatus keskmine, sagedus väike, ebasoovitavate mõjude risk väike.

5.2.3. Majanduslik mõju

Eelnõuga kaasnevad kriitiliste süsteemide varundamisega seotud kulud, mis on detailsemalt lahti kirjeldatud seletuskirja punktis 6.2.

Andmesaatkonna uudne kontseptsioon võib tuua kaudset majanduslikku kasu, arvestades, et lahendus on ka rahvusvaheliselt pakkunud palju huvi ja meediakajastust. Võimalik on luua uus teenus, kus jagatakse teadmisi ja kogemust kontseptsiooni väljatöötamises või võimalik on pakkuda Eesti riigi serveriruume teistele riikidele andmete ja infosüsteemide majutamiseks.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

5.2.4. Mõju elu- ja looduskeskkonnale

Eelnõu muudatused ei too kaasa otseseid või kaudseid mõjusid elu- ja looduskeskkonnale.

5.2.5. Mõju regionaalarengule

Eelnõu muudatused ei too kaasa otseseid või kaudseid mõjusid regionaalarengule.

5.2.6. Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Eelnõuga kaasnev otsene mõju riigi- ja kohaliku omavalitsuste asutustele on minimaalne. Kriitiliste süsteemide vastutavatele töötlejatele võib kaasneda mõningane, kuid mitte märkimisväärne halduskoormuse ja kulude kasv seoses varundamise kohustusega.

Kulude ja halduskoormuse kasv asutustele sõltuvad sellest, kuidas asutused soovivad varunduslahenduse asutuses välja töötada (täiendava riistvara soetamine, manuaalse varundamise või automaatse varundamise valik). Varundamine ei nõua märkimisväärset ümberõpet, lisatööaega ega ka kulusid, sest regulaarne automaatne varundamine kui protsess peaks olema asutustes juba tagatud tulenevalt riigisiseste andmete majutamisele tulenevatest küberturvalisuse nõuetest. Andmesaatkond on täiendav koht, kuhu varundamist teostada.

MKM on valmis koordineerima läbi vajalike partnerite kaasamise asutuste nõustamist ja juhendamist seoses varundamislahenduste väljatöötamisega.

5.2.7. Muud otsesed või kaudsed mõjud

Eelnõu muudatused ei too kaasa muid otseseid või kaudseid mõjusid.

5.3. Kavandatav muudatus: pilvsüsteemi pidamise nõuded

5.3.1. Sotsiaalne, sealhulgas demograafiline mõju

Eelnõuga kaasneb positiivne sotsiaalne mõju. Loodav raamistik pilvandmetöötlusteenuste kasutamiseks tõstab avaliku sektori teenuste usaldusväärsust ja toimepidevust ka siis, kui ülesannete täitmisel tuginetaks välise teenusepakkuja infrastruktuurile.

Ulatus keskmine, sagedus väike, ebasoovitavate mõjude risk väike.

5.3.2. Mõju riigi julgeolekule ja välissuhetele

Eelnõuga kaasneb positiivne mõju riigi julgeolekule. Loodav raamistik võimaldab luua parema ülevaate avaliku sektori teenustest, mis tuginevad pilvsüsteemidele ning nende pidamisel rakendada meetmeid oluliste süsteemide toimepidevuse ning riigi julgeolekut mõjutava teabe konfidentsiaalsuse tagamiseks. Samuti tagab loodav raamistik RIA-le keskse seirevõimekuse avaliku sektori pilvsüsteemide ohtude analüüsimiseks. Kavandatav muudatus pärsib avalikus sektoris pilvandmetöötlusteenuste kasutuselevõtmist nö „moe pärast“ või selle turvalisuse aspekte läbi mõtlemata.

Mõju välissuhetele võib eelnõul olla kahetine. Kuivõrd teenusepakkuja usaldusväärsuse hindamine on suuresti seotud ka teenusepakkuja peakontori jurisdiktsiooni käitumisega, võivad küberruumis agressiivsemad ja demokraatlikest väärtustest mitte lähtuvad riigid panna pahaks teenusepakkuja usaldusväärsuse hindamise nõuet. Samas demokraatlikud riigid, kes Vene Föderatsiooni agressiooni taustal jõuavad järgi Baltimaade arusaamale, et ka küberruumis võtavad vaenulikud riigid kasutusele kõik vahendid, sealhulgas oma tehnoloogiasektori, ning ründavad valimatult nii riiklikke süsteeme kui ka eraettevõtjate teenuseid ja tarneahelaid, saavad võtta eelnõud eeskujuna jõudmaks turvalisema ning raamistatud lähenemiseni pilvandmetöötlusteenuste kasutamisele avalikus sektoris.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

5.3.3. Majanduslik mõju

Eelnõul võib olla majanduslik mõju avalikule sektorile.

Majanduslik mõju Eesti erasektorile ei ole eeldatav, kuivõrd tegemist pole kavandatava muudatuse subjektidega ning Eesti teenusepakkujate äritegevus avaliku sektori suhtes vastab eelduslikult raamistiku nõuetele. Muudatuse eesmärk on ennekõike reguleerida selliste teenusepakkujate teenuste tarbimist, kelle poolt teenuse osutamise reguleerimiseks jurisdiktsioon puudub – nende teenusepakkujate pea- või harukontorid ei asu Eestis.

Avalikule sektorile teeb raamistik kulukamaks pilvandmetöötlusteenuste hankimise, kuid selle kulukuse määr ei ole mõõdetav ning kulukus ei väljendu majandusliku kahjuna.

Raamistiku kulukuse määr avalikule sektorile pilvandmetöötlusteenuste hankimisel ei ole mõõdetav ennekõike põhjusel, et avaliku sektori IKT korraldus on detsentraliseeritud. See tähendab, et ennekõike on asutuse enda otsustada, kui palju ning millise keerukuse süsteeme viimane pilvsüsteemina peab. Peamised nõuded, mis võivad avalikule sektorile majanduslikku mõju avaldada, on:

1) teenusepakkuja usaldusväärsuse hindamise läbiviimise kohustus;

2) kohustus tagada vastu teenusepakkujat riiklikku julgeolekut mõjutava AK teabe konfidentsiaalsus, sh krüpteeritus;

3) kohustus pidada alternatiivseid süsteeme või meetmeid olulise käideldavuse riskiga süsteemide „pilve viimisel".

Esimene nõue võib tekitada subjektile kulu, mis tekib potentsiaalsete teenusepakkujate suhtes usaldusväärsuse hindamise läbiviimisega. Seda mõju vähendab kaks tegurit. Kõigepealt ei nõua teenusepakkuja usaldusväärsuse hindamine tehnilist ekspertiisi osutatavast teenusest. Tegemist on ennekõike teenusepakkuja kui organisatsiooni taustast ja käitumisest tuleneva riskihindamisega, mis on jõukohane ka neile, kel puudub tehniline ekspertiis lahenduse tehnilise turvalisuse hindamiseks. Teiseks on MKM-l kavas levinumate teenusepakkujate suhtes korduvate riskihindamiste tegemise halduskoormuse vähendamiseks luua keskne riskihindamise mehhanism, mille kaudu avalikustataks riskihinnangud levinumate teenusepakkujate suhtes. Variante riskihindamisi teostavateks asutajataks on mitmeid, näiteks muutub üheks suurimaks pilveandmetöötlusteenuste kasutajaks RIT. Samuti saab RIA teha korrakaitseseaduse[39] alusel ohuhinnanguid konkreetse pilveteenuse osutaja suhtes, arvestades siinses paragrahvis olevaid sätteid. Samalaadset analüüsi saab teha ka IT-maja ning selle analüüsi ise avalikustada osas, mis pole juurdepääsupiiranguga. Kavandatav pilvsüsteemi pidamise raamistik jõustub olulise üleminekuajaga ning selle aja jooksul on võimalik keskselt hinnata selliseid teenusepakkujaid, keda Eesti avalikus sektoris laiemalt kasutatakse. Sellest tulenevalt ei tohiks nõue majanduslikult mõjutada ka väiksemaid avaliku sektori subjekte, kelle IKT struktuur piiratud vaid levinumate teenuste kasutamisele.

Teine nõue võib tekitada kulu lahenduste väljatöötamiseks, mis võimaldavad pilvsüsteemis majutatavat või selle kaudu edastatavat AK teavet iseseisvalt krüpteerida. Seda mõju vähendab kaks tegurit. Eelnõus piiritletud krüpteerimise kohustus ainult selgelt riiklikku julgeolekut mõjutava AK teabe suhtes. Valdavale osale juurdepääsupiiranguga töödeldavale teabele ei kohaldu sätestatud AK teabe alused. Tegemist on suures osas teabega, mida töötlevad teabevaldajad turvalisuse kaalutlustel eelduslikult pilvsüsteemis ei hoia või mida töötlevatel teabevaldajatel on valmisolek teabe konfidentsiaalseks töötlemiseks ka pilvsüsteemis. Teiseks on juba praegu võimalik edastada pilvsüsteemide vahel ka teenusepakkuja vastu DigiDoc4 või RIA DigiDoc rakendusega krüpteeritud teavet. MKM-il on kavas ka seoses planeeritava muudatusega arendada kontseptsiooni riiklikust krüptomaterjalist teabe pikaajaliseks majutamiseks pilvsüsteemis krüpteeritud kujul.

Kolmas nõue võib tekitada nõude subjektile kulu, mis tuleneb pilvsüsteemiga paralleelse alternatiivi pidamisest. Seda mõju vähendab kaks tegurit. Esiteks ei kohaldata nõuet kõikidele pilvsüsteemidele, vaid sellistele, mille käideldavuse häirimisel oleks oluline kahjulik tagajärg asutuse tegevusele. Ei saa olla eelduseks, et avalik sektor soovib tugineda pilvandmetöötlusteenustele ehk võõrale infrastruktuurile selliste süsteemide pidamiseks, mille toimepidevus oluliselt avaliku sektori ülesannete täitmist mõjutab, millest tulenevalt on ka meetme mõju piiratum. Teiseks on peetava alternatiivi tehnilised võimekused suuresti subjekti enda määratleda. Peetav alternatiiv ei pea täitma pilvsüsteemi võimekust täielikult, kuid peab

[39] Korrakaitseseadus, RT I, 03.03.2021, 5.

lubama avaliku sektori organisatsioonil jätkata oma ülesannete täitmist ka ilma pilvsüsteemita. Seega varieerub alternatiivi pidamise nõudest tulenev kulu lähtuvalt nii süsteemide mahust ja keerukusest, mida asutus „pilve viia“ soovib, kui ka kaalutlustest alternatiivi enda võimekuste ja arenduste osas.

Kokkuvõtlikult tuleneb raamistiku kehtestamisega kulutusi, mida avaliku sektori organisatsioon süsteemide „pilve viimisel“ kandma peab, kuid kõik peamised majandusliku mõju avaldajad on minimeeritud rakendumaks kas ebatavaliste pilvandmetöötlusteenustele, julgeoleku tagamisega seotud teabele või toimepidevuseks vajalikele süsteemidele.

Täiendavalt ei avaldu raamistiku majanduslik mõju otsese kuluna. Kavandatav regulatsioon rakendub küll pilvsüsteemide pidamisele, kuid ei kohusta ühtki subjekti pilvsüsteemi pidama. Peamine põhjus pilvsüsteemi pidamiseks on aga majanduslik kasu või kokkuhoid võrreldes oma taristul tugineva süsteemi välja arendamise ja hooldamisega. Seega on kavandatava regulatsiooni reaalne majanduslik mõju vaadeldav majandusliku kasu või kokkuhoiu vähendamisena oluliste süsteemide „pilve viimisel“, mitte otsese kuluna subjektile. Mõjusid peab subjekt ennekõike arvestama IKT arenduste eelarve kujundamisel.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

5.3.4. Mõju elu- ja looduskeskkonnale

Eelnõu muudatused ei too kaasa otseseid või kaudseid mõjusid elu- ja looduskeskkonnale.

5.3.5. Mõju regionaalarengule

Eelnõu muudatused ei too kaasa otseseid või kaudseid mõjusid regionaalarengule.

5.3.6. Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Eelnõu ei mõjuta olulisel määral avaliku sektori töökorraldust, kuivõrd kavandatav regulatsioon täiendab, mitte ei kujunda ümber avaliku sektori IKT korralduslikku protsessi. Tekib täiendav vajadus välja töötada sisemine töökorraldus pilvandmetöötlusteenuste pakkujate usaldusväärsuse hindamiseks, kui seda varasemalt tehtud ei ole ning kui soovitakse kasutada pilvandmetöötlusteenuse pakkujaid, keda keskselt hinnatud nimekirjas kajastatud ei ole. Julgeoleku tagamisega seotud AK teabe töötlemisel pilvsüsteemis on ennekõike tehnilise, mitte organisatoorse iseloomuga, sest nimetatud AK teabe määratlemine toimub alustel, mida juba avalikus sektori AK teabe töötlemisel kasutatakse.

Eelnõuga kaasnevad täiendavad kulud järelevalve ja volitusnormide alusel nõuete täpsema tehnilise sisustamise teostamiseks, mis on kirjeldatud seletuskirja punktis 6.3.

5.3.7. Muud otsesed või kaudsed mõjud

Eelnõu muudatused ei too kaasa muid otseseid või kaudseid mõjusid.

6. Määruse rakendamiseks vajalikud kulutused ja määruse rakendamise eeldatavad tulud

6.1. Kavandatav muudatus: E-ITS-i kehtestamine

6.1.1. Küberturvalisuse tagamiseks vajalike kulutuste ja E-ITS-i kehtestamisest tulenevate kulutuste eristamine

Kuigi eelnõu eesmärk on kehtestada uued infoturbe halduse nõuded, siis selle kehtestamisest tuleneva majandusliku mõju analüüsil tuleb eristada E-ITS-i spetsiifikast tulenevaid kulutusi küberturvalisuse tagamiseks tehtavatest kulutustest üleüldiselt. Teenuse osutajad ning enamik isikutest, kellele kohaldatakse teenuse osutajale sätestatud nõudeid, on pidanud küberturvalisuse tagamiseks tegema vastavaid investeeringuid juba kehtiva õiguse (KüTS § 7) alusel.

Mis eristab E-ITS-i varasemalt kehtinud nõuetest, on ennekõike terviklik ja struktureeritud lähenemine küberturvalisuse tagamisele organisatsioonis, ning see, et nende nõuete täitmist on lihtsam kontrollida. E-ITS aga ei kujuta endast kannapööret küberturvalisuse rakendamise põhimõtetes ega parimas praktikas.

On tõenäoline, et E-ITS-i rakendaja hakkab tegema varasemast rohkem investeeringuid küberturvalisusesse, et jõuda vastavusse kehtestatavatele nõuetele ning sealhulgas viia läbi edukas E-ITS-i audit. See aga ei tähenda, et majanduslik mõju E-ITS-i rakendajale tulenes E-ITS-i kehtestamisest – pigem viitab selline olukord, et E-ITS-i rakendaja ei ole varem KüTS-i alusel kehtestatud nõudeid piisavalt põhjalikult järginud.

Seega isegi kui teenuse osutajad ning need, kellele kohaldatakse teenuse osutajale sätestatud nõudeid, peavad tegema olulisi investeeringuid E-ITS-i nõuetele vastamiseks, siis väitmaks, et eelnõu majanduslik mõju on rakendajale suure ulatusega, ei pea rakendaja põhistama, kuidas konkreetsed kulutused on vajalikud E-ITS-i nõuete täitmiseks, vaid just põhistama, kuidas konkreetsed kulutused ei olnud vajalikud kehtiva seaduse nõuete täitmiseks. Küberturvalisuse tagamiseks on vaja teha olulisi pingutusi ja investeeringuid esitatud eelnõust sõltumata.

6.1.2. Küberturvalisuse tagamiseks tehtavate kulutuste majanduslik mõju

Küberturvalisusega seotud kulutused võib jaotada kaheks liigiks – kulutused, mida tehakse küberturvalisuse tagamiseks organisatsioonis (pädeva personali palkamine, teenuste ja süsteemide kaardistamine, riskianalüüs, meetmete rakendamine), ning kulutused, mida tehakse küberintsidendi tagajärgede likvideerimiseks (lunavara nõuded, andmebaaside taastamine, riistvara väljavahetamine, info- ja võrgusüsteemide uuesti arendamine, teenuse osutamata jätmisega tekkinud kahju kandmine (sh esitatud kahjunõuded ja leppetrahvid) jne).

Alati on võimalik, et küberturvalisuse tagamisele olulisi kulutusi teinud organisatsioon ei suuda vältida kahjulikke küberintsidente ega nendega kaasnevaid kulutusi, ning et küberturvalisuse tagamisele kulutusi mitte teinud organisatsioon ei lange küberintsidendi ohvriks ega kanna ka sellest tulenevaid kulutusi, kuid üldreeglina tähendab küberturvalisuse tagamiseks tehtavate kulutuste suurendamine küberintsidendi juhtumise tõenäosuse vähenemist. Samas näitab RIA statistika, millega on võimalik tutvuda iga kuu ilmuva „Olukord küberruumis“ ning kvartaalselt

ilmuva „Trendid ja tähelepanekud küberruumis“[40] väljaande vahendusel, et küberintsidendi ohvriks langemise puhul on küsimus pigem ajas, millal see juhtub, ning milline on toimunud küberintsidendi mõju ulatus. Seega ei saa pidada mõistlikuks lähenemist, et küberturvalisuse tagamiseks jäetakse kulutused tegemata põhjendusel, et loodetavasti organisatsioon ei lange küberintsidendi ohvriks.

Kui eelnõu tulemusel on seetõttu oodatav E-ITS-i rakendajatel ühel või teisel põhjusel (nt varasemalt nõuete ebapiisav täitmine või küberturvalisusega seotud kohustuste puudumine) küberturvalisusele tehtavate kulutuste suurenemist, ei saa seda vaadelda vaid kulutuste kandmise vaatenurgast, vaid tuleb arvestada ka teist liiki kulutuste vältimist. Küberintsidendid on ebaregulaarsed sündmused, mille põhjustajaks on enamasti pahatahtlikud kolmandad isikud, seega ei ole ka otseselt ennustatav suhe, kui palju konkreetne teenuse osutaja küberturvalisuse meetmete rakendamisest majanduslikult võidab või kaotab.

6.1.3. Riigi ja kohaliku omavalitsuse tegevused, eeldatavad tulud ja kulud

Eelnõu rakendamisel kaasneb nii riigi kui ka kohaliku omavalitsuse tasandil ajakulu senise ISKE alusel koostatud dokumentatsiooni vastavusse viimisel E-ITS-iga. E-ITS-i juurutamise etapis tuleb arvestada, et infoturbe rolli täitvatel inimestel kulub põhitöö kõrvalt täiendavalt aega E-ITS-i nõuetega vastavusse viimiseks (aktiivses juurutamise etapis mõned tunnid nädalas).

Eelnõust tulenevalt täiendavate kulutuste tegemise vajadust ei teki, kuivõrd üleminek ISKE-lt E-ITS-i rakendamisele asendab vastavad auditeerimiskulud ning nõuab peamiselt ajalist panust dokumentatsiooni koostamisele.[41]

Küberturvalisuse tagamiseks tehtavate kulutustega tuleb arvestada ka kehtivate õigusaktide alusel, ning kui seni ei ole avalik sektor sellele piisavalt tähelepanu pööranud, siis tuleb avaliku sektori asutusel või muul üksusel selle eest seista oma majandusaasta eelarvestamisel, sh võimaluse korral riigieelarve läbirääkimistel. Asjaolu, et käesolev eelnõu ei too otseselt kaasa kulutuste kasvu kehtivate õigusaktidega võrreldes, ei tähenda, et juriidilisel isikul või asutusel oleks õigustatud küberturvalisuse tagamiseks vajalike kulutuste jätkuv alahindamine.

6.1.4. Järelevalveasutuse tegevused, eeldatavad tulud ja kulud

E-ITS-i kehtestamise eesmärgi raames ei mõjuta eelnõu RIA töökorraldust. Varasem KüTS § 7 lõike 4 alusel kehtestatud nõuete ja ISKE nõuete järgimise kontroll asendub E-ITS-i nõuete järgimise kontrolliga.

RIA töökoormust võib eelnõu suurendada suurema hulga auditite järeldusotsuste ülevaatamise vajaduse tõttu. Samuti on vajalikud täiendavad toetustegevused E-ITS edasi arendamiseks ning KüTS-i subjektidele vastavate profiilide loomiseks.

[40] Leitav: https://www.ria.ee/et/uudised.html?type-filter[0]=Olukord%20k%C3%BCberruumis.
[41] Siin on abiks vastavad abimaterjalid (sh üleminekujuhend ISKE-lt E-ITS-le), mis on leitavad E-ITS-i portaalist: https://eits.ria.ee/

RIA esmase hinnangu kohaselt on järelevalve eesmärkide täitmiseks vajalik palgata juurde kolm töötajat ning E-ITS arendamiseks ja profiilide loomiseks täiendavalt kolm töötajat. Personali- ja halduskulude arutelu toimub riigi eelarvestrateegia protsessis.

6.2. Kavandatav muudatus: avalike ülesannete täitmist oluliselt mõjutavate süsteemide pidamise nõuded

Kuivõrd Luksemburgi andmesaatkond on juba käivitatud ning andmeid ja infosüsteeme on varundatud alates 2019. aastast, siis on selle käitamiseks vajalikud tehnilised lahendused Registrite ja Infosüsteemide Keskuse (edaspidi *RIK*) poolt välja töötatud ning serveriruum vastava riist- ja tarkvaraga sisustatud. Andmesaatkonna rendikulud Luksemburgiga sõlmitud rahvusvahelise lepingu alusel on 236 000 eurot aastas, mille tarbeks on MKM-ile raha eraldatud riigieelarvest kuni nimetatud lepingu kehtivuse lõpuni (31.12.2022). Lisaks üüritasule kaasnevad andmesaatkonna pidamisega ka serveriruumi elektritarbimise kulud, mille tasumiseks eraldas MKM lepingu alusel RIK-le, kui serveriruumi haldus- ja majutusteenuse osutajale raha kuni eelnimetatud lepingu lõppemiseni. Eelnõu koostamise hetkeks on RIK-lt vastava ülesande üle võtnud RIT.

Asutustel ei teki märkimisväärseid varundamisega seotud kulusid eeldusel, et varundamise protsess juba toimib. Reeglina on asutustes juba tulenevalt ISKE nõuetest kasutusele võetud andmete riigisisese regulaarse andmevarunduse osas toimiv protsess. Andmesaatkond on täiendav koht, kuhu varundamist teostada. Kulude kasv asutustele sõltub sellest, kuidas asutused oma varunduslahendused soovivad välja töötada (täiendava riistvara soetamine, manuaalse varundamise või automaatse varundamise valik). Varundamisega seonduvad halduskulud kaetakse asutuste eelarvest.

6.3. Kavandatav muudatus: pilvsüsteemi pidamise nõuded

Eelnõu ei eelda rakendamisega kaasnevaid olulisi majanduslikke kulutusi raamistiku subjektidele, ennekõike vähendab raamistik pilvandmetöötlusteenuste kasutamise majanduslikke eeliseid pilvsüsteemi turvalisuse tagamise eesmärgil.

Juba kasutatavate pilvandmetöötlusteenuste kooskõlla viimine kavandatavate muudatustega võib tekitada kulutusi, mille ulatus sõltub muidugi kasutatavate teenuste mahust, kuid millega peamised kaasnevad muutused tegevustes on siiski tehnilised ümberkorraldused ja dokumentatsiooni vormistamised. Sellega kaasneva ajakulu arvestamiseks jõustub kavandatav regulatsioon ka 2024. aasta alguses.

Järelevalve teostamiseks on RIA esmasel hinnangul vajalik palgata juurde kuni 8 töötajat. Täpsemalt:

1) Kuni viis töötajat pilvsüsteemide logide seire teostamiseks, st kuni kolm töötajat aktiivse seire teostamiseks, üks töötaja logilahenduste haldamiseks ning üks töötaja järelevalve süsteemide arendamiseks. Vajalike kulutustega kaasneks ka ligikaudu poole miljoni ulatuses majanduskulu ning saja tuhande ulatuses investeeringute kulu.

2) Kuni kolm töötajat nõuete üle järelevalve teostamiseks.

Personali- ja halduskulude arutelu toimub riigi eelarvestrateegia protsessis.

7. Määruse jõustumine

Määrus jõustub 531 SE-ga samal kuupäeval, kuid mõne erisusega.

Määruse §-id 7 kuni 11 jõustuvad 1. jaanuaril 2023. a. Tegemist on andmekogude suhtes ISKE-lt E-ITS-le vormistusliku ülemineku võimaldamise normidega, mis jõustuvad samal ajal ISKE kehtetuks tunnistamisega. Need muudatused toimuvad 531 SE tõttu AvTS-i muudatustega.

Määruse §-id 14 kuni 19 jõustuvad 1. jaanuaril 2024. a. Tegemist on pilvsüsteemi pidamise nõuete sätetega, mille suhtes rakendatakse üleminekuaega olemasolevate pilvsüsteemide kooskõlla viimiseks.

8. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu on seotud Riigikogus arutatava seaduseelnõuga ehk 531 SE-ga. 531 SE avaliku kooskõlastuse käigus (toimus viimati sügisel 2021. a) esitati ka kommentaare ja märkusi teemade kohta, mis on pigem seotud siinse eelnõuga. Need märkused koos eelnõu koostajate uuendatud vastustega on lisatud seletuskirjale kui lisa 2, et hõlbustada siinsele eelnõule kooskõlastuse andmist või arvamuse avaldamist.

Eelnõu esitati kooskõlastamiseks eelnõude infosüsteemi kaudu kõikidele ministeeriumitele ning arvamuse avaldamiseks põhiseaduslikele institutsioonidele, avalik-õiguslikele juriidilistele isikutele, Andmekaitse Inspektsioonile, RIA-le, Keskkonnaministeeriumi Infotehnoloogiakeskusele, RIK-le, RIT-le, Rahandusministeeriumi Infotehnoloogiakeskusele, Siseministeeriumi infotehnoloogia- ja arenduskeskusele, Tervise ja Heaolu Infosüsteemide Keskusele, Eesti Linnade ja Valdade Liidule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Infosüsteemide Audiitorite Ühingule ning RIA vahendusel elutähtsate ja oluliste teenuste osutajatele.