



LEXTAL

TALLINN • RIGA • VILNIUS



ÕIGUSANALÜÜS RIIGIPILVES ANDMETE MAJUTAMISE KOHUSTUSLIKKUSE ÕIGUSLIKU KONTSEPTSIOONI KUJUNDAMISEKS

KOKKUVÕTE

Tellija: Majandus- ja Kommunikatsiooniministeerium

Täitja: Advokaadibüroo LEXTAL OÜ

11. august 2023

1. EELSÖNA

1. Advokaadibüroo LEXTAL (edaspidi ka **meie**) kliendiks on Majandus- ja Kommunikatsiooniministeerium (registrikood 70003158; edaspidi: **MKM**), kelle palvel on koostatud õigusanalüüs riigipilves andmete majutamise kohustuslikkuse õigusliku kontseptsiooni kujundamiseks (edaspidi: **Õigusanalüüs**).
2. MKM ja tema hallatava Riigi Info- ja Kommunikatsioonitehnoloogia Keskuse (edaspidi: **RIT**; MKM ja RIT edaspidi koos: **Tellijad**) eesmärk on koondada Eesti avaliku sektori killustunud server-baastaristu kesksesse asutusse. Selle saavutamiseks on üks võimalik lahendusvariant muuta riigi poolt hallatava pilvekeskkonna ehk riigipilve (edaspidi: **riigipilv**) kasutamine avalikus sektoris kohustuslikuks.
3. Õigusanalüüsi eesmärgiks oli hinnata regulatiivseid võimalusi lähtuvalt õiguslikest kaalutlustest andmete riigipilves majutamiseks kohustamisel. Seejärel hinnata, millised mõjud toob kaasa riigipilve kasutamise kohustuslikuks muutmine. Analüüsi uurimisesemesse kuulusid muuhulgas järgnevad õiguslikud küsimused:
 - a) Kui riigipilve kasutamine oleks kohustuslik, siis kas kasutamise kohustuslikkus võiks olla määratletud objektidele (andmekogud või infosüsteemid) või subjektidele (riigiasutused, kohalike omavalitsuste asutused, eraõiguslikud juriidilised isikud, kes täidavad avalikke ülesandeid)?
 - b) Kas RIT riigipilve haldajana vastutab andmekogu vastutava töötaja eest infoturbenõuete täitmise osas täies ulatuses, kui riigipilv oleks kohustuslik?
 - c) Kas RIT muutub andmekogudes sisalduvate isikuandmete volitatud töötajaks, kui andmekogu vastutav töötaja andmed riigipilve majutab?
4. Õigusanalüüs koostati informatsiooni põhjal, mida Tellijad on avaldanud meile enne Õigusanalüüsi koostamist ja selle käigus. Õigusanalüüsis sisalduv analüüs põhineb Õigusanalüüsi kuupäeval jõus olevatel õigusaktidel (v.a kui Õigusanalüüsis on vastupidiselt sedastatud). Juhime tähelepanu, et Õigusanalüüsis sisalduv analüüs on meie tõlgendus kohaldatavatest õigusaktidest ning see ei pruugi ühtida ametiasutuste ja kohtute tõlgendusega.
5. Käesolev dokument on Õigusanalüüsi kokkuvõte (edaspidi: **Kokkuvõte**). Kokkuvõttes on toodud Õigusanalüüsis esitatud peamised järeldused ja soovitusel ning see on mõeldud Õigusanalüüsi lugemise lihtsustamiseks. Kokkuvõte ei ole eraldiseisev dokument, see sisaldab viiteid Õigusanalüüsile, selles on kasutatud Õigusanalüüsis defineeritud mõisted ning palume seda lugeda koos Õigusanalüüsiga.

2. PEAMISED JÄRELDUSED

2.1. Kohustuslikkuse määratlemise alused

Riigipilve kasutamise kohustuslikkus tuleks reguleerida läbi reguleerimisala (objekt ehk milliseid infosüsteeme riigipilves majutada tuleks) ning kohaldamisala (subjekt ehk kelle infosüsteeme riigipilves majutada tuleks) kombinatsiooni.

6. Kui just puudub eesmärk kehtestada riigipilve kasutamise kohustust üksikute infosüsteemide suhtes (või välistada üksikud infosüsteemid), tuleks kohustuse objekti ja subjekti defineerida iseseisvalt.
7. Kohustusliku infosüsteemide majutamise kontseptsiooni väljatöötamisel tuleks vältida riigipilve defineerimist. Kohustuslikkuse sõnastamisel tuleks vältida subjekti kohustuse (nt „X peab Y-t majutama riigipilves“) põhist lähenemist, sest sellega kaasneks „riigipilve“ defineerimise problemaatika ning sõltumata riigipilve käsitlusest toote või teenusena tekiks mõiste kasutamisel sõnastuslik takistus kohustuslikkuse kontseptsiooni muude osade kavandamisel.
8. Põhjendatum oleks sõnastada kohustuslikkus läbi RIT-le avaliku ülesande kehtestamise nii infosüsteemide majutamiseks kui ka majutamiseks kasutatavate ressursside (sh pilvandmetöötlusteenuste) koondamiseks.

2.2. Kohustuslikkuse sisuline ulatus

Kohustuse objekt (ehk mida riigipilves majutatakse) peaks tuginema võimalikult laiatähenduslikule mõistele (nt „võrgu- ja infosüsteem“).

9. Täpset kohustuse objekti on seejärel võimalik piiritleda täiendavate mõistetega, mis võimaldavad eristada majutamisele kuuluvaid tehnoloogiate liike ning välistada samaliigiliste tehnoloogiate hulgast süsteemid, mille funktsioonidest tulenevalt riigipilves majutamine oluline ei ole.
10. Objekti kitsendused peaksid tuginema nii tehnoloogilistele kui ka funktsionaalsetele mõistetele. Tehnoloogilise mõistega kitsendus (nt „andmetöötlusressursid“ KÜTS tähenduses) võimaldab eraldada tehnoloogia, mida RIT haldab (ja ka koondab ülesande täitmiseks) tehnoloogiast, mida RIT majutab. Funktsionaalse mõistega kitsendus (nt „otsese avaliku teenuse“ osutamiseks kasutatav süsteem TKTA tähenduses) võimaldab välistada objektist samaliigilised tehnoloogiad, mille riigipilves majutamine oluline ei ole.

Kohustuse subjektide määratlus (ehk kelle infosüsteeme majutatakse) tuleks piiritleda valitsusasutustele ja valitsusasutuste hallatavatele asutustele.

11. Finantsgarantii, ettevõtlusvabaduse ning riigiabi õigusvaldkonnad võivad mõjutada kehtestatava kohustuse seaduspärasust, kui subjektide ringi kaasata kohaliku omavalitsuse üksused või muud avalikke ülesandeid teostavad juriidilised isikud. Vastavate subjektide kaasamise seaduspärasus sõltuks kohustuse täpsemast sõnastusest ning vajaks vastavalt täiendavat õigusanalüüsi. Lisaks, kohustuse seadmine laiemale subjektide ringile ei pruugi olla praktikas teostatav.

Kohustuslikkuse sisuline ulatus peab võimaldama subjektil kehtestada tehnilised tingimused, mida RIT peab järgima infosüsteemi majutamisel.

12. See kriteerium tagab, et RIT-i volitused ülesande täitmisel ei sekku subjekti valitsemisala korraldamisse ehk RIT ei hakka avalikku teenust koos subjektiga korraldama. Sellest tulenevalt jääb RIT isikuandmete ja teabe (AvTS tähenduses) volitatud töötlejaks ning ei teosta täidesaatvat riigivõimu subjekti suhtes. RIT võib korraldada majutamise tehnilisi tingimusi ulatuses, mis ei ole vastuolus subjekti kehtestatud nõuetega.

2.3. Kohustuslikkuse reguleerimiseks sobiv õigusakt

Kohustuse kehtestamiseks sobivad õigusaktid on KüTS, TKTA määrus või eraldiseisva seaduse koostamine.

13. Kohustuslikkusega seonduvate aspektide reguleerimiseks sobiv õigusakt peab vastama kahele kriteeriumile. Õigusakti kohaldamisala peab hõlmama soovitud subjektide ringi ning õigusakti reguleerimisala peab käsitlema infosüsteemide haldamist.
14. Kohustuse kehtestamiseks üheks sobivaks variandiks on eraldiseisva seaduse koostamine.
15. Teiseks variandiks on küberturvalisuse seadus. Selle seaduse kohaldamisala hõlmab tervet avalikku sektorit ning reguleerimisala käsitleb nõudeid infosüsteemide haldamisele. Peamine mõttekoht on see, et sätted peavad kandma küberturvalisuse tagamise eesmärki. Tsentraalne infosüsteemide majutamine koondatud vahenditega sellist mõju samas ka saavutaks.
16. Kolmas variant on TKTA määrus. TKTA-l on oluline eelis teiste variantide ees, sest TKTA reguleerimisala pakub ka asjakohast lahendust objektide funktsionaalseks piiritlemiseks. Nimelt võimaldaks TKTA alusel tehtav regulatiivne lähenemine kitsendada majutatavate infosüsteemide ringi selliste infosüsteemide peale, mida kasutatakse otsese avaliku teenuse osutamiseks TKTA tähenduses. Vältimaks TKTA kohaldamisalaga seotud vaidlusi ja õigusselguse tagamiseks tuleks TKTA lahendusvariandi kasutamise korral sätestada ka volitusnorm seaduses (nt KüTS-s).

2.4. Infoturbenõuetest tulenevalt vastutused ja kohustused

Nii RIT kui ka subjekt vastutavad infoturbenõuete täitmise eest vastavalt kontrolli teostamise ulatusele majutatava infosüsteemi või selle osade suhtes.

RIT ja subjekt eraldiseisvalt on kohustatud täitma infoturbenõudeid ennekõike nende süsteemide osas, mida nad faktiliselt kontrollivad. Tsentraliseeritud majutamise puhul on majutatavale infosüsteemile riskianalüüsi teostamise ja turvameetmete rakendamise kohustus jaotatud RIT-i ja subjekti vahel lähtuvalt sellest, millises ulatuses infosüsteemi (kui infovarade kogumiku) üle kumbki osapool faktilist kontrolli teostab. Täpne jaotus määratletakse igakordselt kaitseala määratlemisel kummagi organisatsiooni poolt. Mõnikord võivad RIT ja subjekt kaardistada sama infovara oma vastavasse kaitsealasse. Kuivõrd RIT ja subjekt ei täida dubleerivaid ülesandeid, siis peaks see reeglina aga tähendama erinevaid riskide kaardistusi ja vastavalt eraldiseisvat riskihaldust.

Subjektile kohaldub vastutus infoturbemeetmete rakendamise eest RIT-i poolt KÜTS § 7 lg 3 alusel. Selle kohustuse täitmise võimaldamiseks peab kohustusliku majutamise kontseptsioon võimaldama subjektil edasi anda infoturbelist informatsiooni majutatavast infosüsteemist, mida RIT peab arvesse võtma ning millest lähtuvalt sihtobjektide riskihaldust vajadusel korrigeerima.

17. KÜTS § 7 lg 3 ning 8 lg 11 alusel tekib subjektile nn tarneahela vastutus ka RIT suhtes, sest subjekt volitab süsteemi haldamise teisele isikule või majutab seda teise isiku juures KÜTS § 7 lg 3 tähenduses. Kuid see vastutus ei ole samatähenduslik kohustusega ise turvameetmeid andmetöötlusressurssidele rakendada.
18. Tavapärase pilvandmetöötlusteenuse etalon-turbemeetmed ei ole kohaldatavad seadusliku kohustuse olemasolul riigipilve kasutamiseks. Subjekti jaoks aga meetmete puudumine KÜTS § 7 lg 3 kohustuse täitmiseks tekitab küberturvalisuse kontekstis ohtliku olukorra, kuivõrd RIT ei pruugi ka nõuetekohase turvameetmete rakendamisel arvestada subjekti majutatava süsteemi kaitsetarbega.
19. Lahendusena tuleb subjektile kohustusliku riigipilve kontseptsiooni kavandamisel luua instrument KÜTS § 7 lõikes 3 sätestatud kohustuse täitmiseks RIT-i suhtes, mis võimaldab subjektil edasi anda infoturbelist informatsiooni majutatavast infosüsteemist, mida RIT peab arvesse võtma ning millest lähtuvalt sihtobjektide riskihaldust vajadusel korrigeerima.

2.5. Andmekaitse nõuetest tulenevalt vastutused ja kohustused

Reeglina jääb infosüsteemi majutamise korral subjekt isikuandmete vastutava töötaja rolli ning RIT isikuandmete volitatud töötaja rolli. Subjektile peaks jääma pädevus kehtestada RIT-le tehnilisi tingimusi infosüsteemi majutamiseks, mis muuhulgas tähendaks seda, et subjektil on võimalik otsustada, kas majutamine RIT-i poolt hõlmab isikuandmete töötlemist või mitte.

20. Subjekt töötleb isikuandmeid samas mahus, mis kehtiva regulatsiooni kohaselt ning sellele lisandub vaid RIT-le (või pilveandmetöötlus teenusepakujale) isikuandmete edastamise toiming.
21. RIT töötleb isikuandmeid eelkõige infosüsteemi majutamise raames, kuid töötlemise toiminguid võib esineda erandlikel juhtudel ka infosüsteemi haldamise raames.
22. Ulatuses, kus subjekt edastab RIT-le pseudonüümitud isikuandmeid või RIT-i puudub ligipääs isikuandmetele, ei töötle RIT isikuandmeid ning talle ei teki andmekaitse nõuetest tulenevalt vastutusi ja kohustusi.
23. Subjekt on eraldiseisev vastutav töötaja ulatuses, kus ta töötleb isikuandmeid tema pädevusse antud otsese avaliku teenuse või tugiteenuse täitmiseks ning olukordades, kus subjekt on vastutav töötaja kehtiva regulatsiooni kohaselt, jääb ta vastutavaks töötajaks ka kohustuslikkuse järgselt.
24. RIT vastab eelkõige volitatud töötaja tunnustele isikuandmete osas, mille subjekt talle edastab. Sellist järeldust kinnitaks ka see, kui subjektil on teatud ulatuses pädevus mõjutada isikuandmete majutamise viisi. Subjekti pädevus kehtestada RIT-le tehnilisi tingimusi infosüsteemi majutamiseks võimaldaks subjektil otsustada, kas majutamine RIT-i poolt hõlmab isikuandmete töötlemist või mitte. Isikuandmete töötlemise volituse andmise korral peaks kohustuse kontseptsioon

sätestama korra, mille alusel subjekt RIT-i volitab (sh määrab töötlemise eesmärgid, ulatuse, tehnilised meetmed jne).

2.6. Avaliku teabe juurdepääsu nõuetest tulenevalt vastutused ja kohustused

RIT ei ole teabevaldaja sellise avaliku teabe osas, mille ta on saanud subjektilt majutamiseks.

25. Subjekt on teabevaldaja sellise avaliku teabe suhtes, mille ta on saanud või loonud avalikke ülesandeid täites. See hõlmab ka teavet, mida majutab RIT ning kohustuslikkuse järgselt subjekti kohustused ja vastutused teabevaldajana ei muutu ka tulenevalt sellest, et osa teavet on majutatud RIT-i juures.
26. RIT on teabevaldaja avaliku teabe osas, mille ta on saanud või loonud oma avalikke ülesandeid täites, eelkõige infosüsteemi haldamise raames ja pilveteenuse hankimise raames. See ei hõlma teavet, mille RIT on saanud subjektilt majutamiseks ning vastava teabe osas ei ole RIT teabevaldaja.

Reeglina jääb infosüsteemi majutamise korral subjekt andmekogu vastutava töötaja rolli ning RIT volitatud töötaja rolli.

27. Osas, kus RIT majutab subjekti andmekogu infosüsteemide majutamise ülesande raames, on subjekt vastava andmekogu vastutav töötaja ja RIT vastava andmekogu volitatud töötaja.

AK-teabele saab juurdepääsuõiguse anda vaid sellisele RIT-i teenistujale, kellel on juurdepääsuõigust oma ametiülesannete täitmiseks vaja.

28. Nii subjektil kui RIT-il tekib juurdepääs AK-teabele. RIT täidaks avalikku ülesannet, milleks on mh infosüsteemide majutamine. Osas, kus infosüsteemide majutamiseks on RIT-i töötajal vaja juurdepääsu majutatavale AK-teabele (nt majutamine ilma juurdepääsuta pole tehniliselt võimalik), siis vastab RIT-i teenistuja AvTS § 38 lg-s 3 nimetatud riigi ametnikule või teenistujale, kellel on juurdepääsuõigus AK-teabele. AK-teabele saab seega juurdepääsuõiguse anda vaid sellisele RIT-i teenistujale, kellel on juurdepääsuõigust oma ametiülesannete täitmiseks vaja.

3. EDASISED SAMMUD

Volitatud töötleja ja vastutava töötleja rollijaotus isikuandmete töötlemisel ja andmekogude majutamisel sõltub kohustusliku riigipilve kontseptsiooni kavandamisel tehtavatest õiguslikest valikutest. Tellijad peavad seega otsustama, kas alustada kohustusliku riigipilve kontseptsiooni kavandamist ning kui jah, siis millises ulatuses.

29. Õigusanalüüsi järeldused, et RIT on ülesannete täitmisel isikuandmete või avaliku teabe volitatud töötleja (ja mitte vastutav), põhinevad hüpoteetilistel regulatiivsetel valikutel, mida seadusandja selle tulemuse saavutamiseks peaks ellu viima.
30. Peamine regulatiivne valik, mida seadusandja peaks tegema, on see, et avaliku ülesande sõnastus RIT-le ei hõlmaks isikuandmete ega avaliku teabe töötlemist. See saab juhtuda kasutades ära nn ümbrikuefekti ja võimalikult suurel määral majutamise tehniliste tingimuste määramise õiguse andmisega subjektile.
31. Tagajärjena oleks soovitatav ka reguleerida isikuandmete ja AK-teabe volitamise kord subjektilt RIT-le. Sedasi saab subjekt sisustada volituse tingimusi, mis on RIT-le järgimiseks kohustuslikud ning seega saab volitus olla ka seaduspärane.
32. Nende regulatiivsete valikute mitte tegemisel seadusandja poolt eksisteerib võimalus, et RIT-i tuleks käsitleda isikuandmete ja/või avaliku teabe vastutava töötlejana oma ülesannete täitmisel.
33. Õigusanalüüsis esitatud järelduste kohaldatavus sõltub seega ennekõike kriteeriumitest, mis võimaldavad subjektil kehtestada tehnilisi tingimusi RIT-le infosüsteemide majutamisel. Samuti nõuab toimiv lahendus teabevahetust subjekti poolt majutatava infosüsteemi kaitsetarbe osas RIT-le.
34. Tellijad peavad seega esmajärgus otsustama, kas alustada kohustusliku riigipilve kontseptsiooni kavandamist ning kui jah, siis millises ulatuses. Oleme andnud soovitusel kohustuslikkuse objektide määratlusele ning subjektide ringile.

Kontseptsiooni kavandamine eeldab seaduseelnõu väljatöötamiskavatsuse koostamist.

35. Oleme selleks otstarbeks koostanud ka regulatiivse lahenduse näidise, mis lähtus Õigusanalüüsi teostamise kestel läbiviidud koosolekutest ja ootuste kaardistustest (leitav Õigusanalüüsi peatükist 7.2).
36. Vastav lahendus lähtub järgnevatest otsustest kohustusliku riigipilve skoobi subjektide ja objektide osas: a) subjektid – valitsusasutused ja valitsusasutuste hallatavad asutused VVS § 38 mõistes; b) objektid – otseste avalike teenuste ja tugiteenuste osutamiseks kasutatavad infosüsteemid TKTA määruse tähenduses.
37. Lahendusvariandi tehniline tähendus hõlmab kahepoolset ülesannet RIT-le: esiteks koondada enda halduse alla kõik riigiasutuste andmetöötlusressursid ning teiseks majutada kõik riigiasutuste infosüsteemid (sealhulgas andmed) nende andmetöötlusressursside või pilvandmetöötlusteenuste peal.

Optimaalne ajaline raamistik näeb ette kontseptsiooni rakendamist praktikas kõige varasemalt 2027. aasta I kvartalis.

38. Teekaardi etapid koos hinnangulise ajaraamistikuga on toodud Õigusanalüüsi alapeatükis 7.1. Selline tegevuskava eeldab iga menetlusetapi lõpuleviimist ühe kuni kahe kvartali jooksul ning üleminekuaja kehtestamist vähemalt ühe aasta ulatuses. Tegemist on optimistliku prognoosiga, mille põhiraskus on võimalikult

kiiresti väljatöötamiskavatsuse koostamisel, et anda mõistlikult aega mõjutatud asutustele seisukohtade kujundamiseks.

/allkirjastatud digitaalselt/	/allkirjastatud digitaalselt/	/allkirjastatud digitaalselt/	/allkirjastatud digitaalselt/
Rauno Kinkar	Henri Ratnik	Oliver Grauberg	Dan-Erik Roosve
vandeadvokaat, partner	vandeadvokaat	advokaat	advokaat