Eesti riigipilve kontseptsioon

Majandus- ja Kommunikatsiooniministeerium, 2015

Sisukord

Resümee

Eesti infoühiskonna arengu tagamiseks on tehnoloogialahenduste pidev kaasajastamine möödapääsmatu. Seetõttu on riigil vaja investeerida muu hulgas ka pilvetehnoloogiasse ja –lahendustesse. Pilvetehnoloogia soodustab ressursside efektiivsemat kasutamist (võimaldab kokkuhoidu nii riist- ja tarkvara investeeringutelt kui ka inimressursilt), on energiasäästlik ja keskkonnasõbralik, ühtlustab teenuste kvaliteeti, toetab innovatsiooni ja uute tehnoloogiliste lahenduste kiiret kasutuselevõttu ning võimaldab asutustel kasutada serverimajutuse tehnoloogia tippeksperte.

Eesti infoühiskonna järjepidevuse toetamiseks kavandatav Eesti riigipilv on hübriidpilv, mis kätkeb endas riigiasutustele osutatavat privaatpilve teenust, erasektori poolt opereeritavaid avalikke pilvi ning välisriikides paiknevaid andmesaatkondi. Riigi privaatpilve tekkeks on vaja rajada üks kõrgturvaline riiklik andmekeskus, mis tagaks kõrgkäideldavuse ja kvaliteetse pilveteenuse pakkumise ning kataks ära riigiasutuste majutusressursside vajaduse. Dubleeriva andmekeskuse rajamisel on samuti oluline selle asukoht, mis peab jääma Tallinna piirkonnast välja, et suurendada turvalisust, võimaldades riigiasutustel majutada oma andmed ja infosüsteemid hajusamalt.

Riigipilve rajamine hoiab IT kulud riigi-üleselt praegusel tasandil, siiski riigiasutused peavad arvestama, et riigipilve teenuse eest tekib neil eelarvesse uus kulurida, mida nad riigipilve teenuse osutajale peavad maksma. Samas pilvetehnoloogia võimaldab paindlikkust, mis on oluline e-teenuste kvaliteedi tõstmiseks ja ressursside efektiivsemaks kasutamiseks.

Eesti riigipilve lahendus tagab digitaalse järjepidevuse, maandab infotehnoloogilised riskid, suurendab infoturbe võimekust, aitab kaasa innovaatiliste ja kvaliteetsete e-teenuste arendamisele, võimaldab üles ehitada nn „piirideta riigi“ ja tõstab kulu-efektiivsust. Samuti on oluline riigile tekitada suutlikkus kasutada pilvetehnoloogiat oma süsteemide ülesehitamisel ja parendamisel, selleks peavad uued arendatavad infosüsteemid lähtuma pilvetehnoloogia kasutamist soosivatest printsiipidest. Riigipilve lahenduse laialdast kasutuselevõttu toetavad Eesti hajutatult paiknev IT arhitektuur ja turvalise andmevahetusplatvormi kasutamine, kusjuures oluline on, et serveriressurss ei paikneks füüsiliselt ainult Eesti territooriumil, vaid asuks ka väljaspool Eestit ning Eesti riik oleks suuteline pakkuma kriitilisi e-teenuseid igas olukorras.

Ehkki riigipilve põhimõtete osas ei erine Eesti teistest riikidest märkimisväärselt, toob meie sõltuvus IKTst endaga kaasa riigipilve laialdasema kasutuselevõtu ning võimaldab paremini kasutada pilvetehnoloogia eeliseid.

Sissejuhatus

Käesoleval ajal on pilvetehnoloogia järjest kasvava tähtsusega valdkond ning IT infrastruktuuri arengus üks olulisemaid suundi. Erinevates uuringutes, analüüsides ja Euroopa Liidu institutsioonide seisukohtades on kokkuvõtlikult järeldatud, et pilvandmetöötlus suurendab teenuste osutamises paindlikkust, hõlbustab organisatsioonidel teenusepakkujate kaudu uutele ressurssidele ligipääsu ning võimaldab lihtsate vahenditega oma IT funktsionaalsust ja võimekust suurendada.[1] Pilvandmetöötluse kasutegur nii avaliku- kui erasektori jaoks seisneb ressursside efektiivsemas kasutamises ja paindlikkuses, aga ka uute lahenduste väljatöötamis- ja testimisprotsessi kiirendamises ning innovatsiooni võimaldamises. Mitmed riigid - näiteks Ameerika Ühendriigid, Ühendkuningriik, Holland[2], Hispaania, Prantsusmaa, India ja Hiina, kuid ka Põhjamaad on oma avaliku sektori tarbeks pilvandmetöötluse väljaarendamist alustanud. Seega on avalik sektor terves maailmas teadvustanud, et pilvandmetöötlus suudab pakkuda paremaid teenuseid väiksemate ressurssidega.

2012. aasta septembris võttis Euroopa Komisjon vastu strateegia pilvandmetöötluse võimaluste kasutamiseks Euroopas ("*Unleashing the Potential of Cloud Computing in Europe*").[3] Strateegia toetab pilvandmetöötluse kasutuselevõttu kõigis majandussektorites ning pilvetehnoloogia abil loodetakse saavutada Euroopa Liidu 2020. aastaks iga-aastaseks SKT kasvuks 160 miljardit eurot (ligikaudu 1%). Pilveandmetöötluse kasutuselevõttu kajastavate allikate kohaselt sõltub sellest juba mõne aasta pärast ligi 80% ettevõtetest.[4]

Ehkki käesoleval ajal on nende prognooside paikapidavust veel vara hinnata ning rääkida kulude kokkuhoiu, utiliseerimise ja tõhususe kasvu, skaleeritavuse ja teenuste parema kättesaadavuse saavutamisest tänu virtualiseerimisele on siiski ilmne, et Euroopa Liidu liikmesriikide jaoks on pilvandmetöötlus tohutu potentsiaaliga valdkond. Hiljutiselt on selle vajalikkust rõhutatud muu hulgas näiteks ka Euroopa Komisjoni digitaalse ühtse turu strateegias.[5] Pilvetehnoloogia kasutamist tuuakse ühe e-riigi lähituleviku trendina välja ka Eesti Infoühiskonna arengukavas 2020.[6]

Riigipilve kontseptsiooni koostamisel tuli tõdeda, et Eesti riigi pilvandmetöötluse vajadused ning nõuded erinevad teiste liikmesriikide omadest ning Eesti kõrget IKT arengutaset arvestades on kavandamisel oleva Eestil riigipilve kasutusala võrreldes mitmete liikmeriikidega laiem.
Erinevatest uurimustest ja kontseptsiooni koostamisele eelnenud intervjuudest ekspertidega on koorunud välja rida põhjusi, miks Eestile oleks riigipilve vaja ning millistele aspektidele selle loomisel tuleks tähelepanu pöörata.

---

[1] KPMG „Cloud Strategies for Public Sector in Central and Eastern Europe" 2013, kättesaadav: http://www.kpmg.com/EE/et/IssuesAndInsights/ArticlesPublications/Pressiteated/Documents/Cloud%20Strategies%20for%20Public%20Sector%20in%20CEE%20WEB.pdf.

[2] Holland on viinud läbi riiklikke andmekeskuste konsolideerimise, misläbi on vähenenud kulutused riistvarale 40% ja personalikulud 30%. Pilvetehnoloogia kasutusele võtuga loodavad nad kulutusi jätkuvalt vähendada.

[3] European Commission, "European "Cloud Computing Strategy" 2013, kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF.

[4] ENISA "Good Practise Guide for securely deploying Governmental Clouds." 2013, kättesaadav: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds

[5] European Commission „A Digital Single Market Strategy for Europe" , kättesaadav: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

[6] „Infoühiskonna Arengukava 2020", kättesaadav: http://infoyhiskond.eesti.ee/files/Infoyhiskonna_arengukava_2020

Nende põhjal on riigipilve rajamise peamised eesmärgid kokkuvõtlikult järgmised:

1) maandada riigiasutuste riistvaralise taristuga seotud IT riske, sest käesoleval ajal pole paljude riigiasutuste serveriruumide turvalisuse tase piisav, kuivõrd serveriruumide füüsilised riskid, infosüsteemide käideldavuse ja - töökindluse riskid pole alati maandatud;
2) toetada laiapõhist riigikaitset, kuivõrd Eesti riigi püsimajäämine ning katkematu ja tõrgeteta toimimine digitaalselt sõltub üha enam andmete ja avalike teenuste kättesaadavusest;
3) parendada kompetentsi, mis tegeleb infosüsteemide majutuse ja haldamisega, sest riigipilve rajamisega ja serveriressursside konsolideerimisega koonduksid kokku ka valdkonna tippspetsialistid ning lihtsustuks uute inimeste värbamine (kaoks riigiasutuste vaheline konkurents pädevate inimeste pärast ja samuti tippspetsialistid tahavad koos töötada oma valdkonna tippudega);
4) toetada e-residentsuse levikut ja seeläbi majanduskasvu nii siseriiklikult kui piiriüleselt;
5) suurendada avaliku sektori asutuste infoturbe võimekust, kuivõrd turvanõuete täitmine on käesoleval ajal asutuseti erinev ja sageli ebapiisav;
6) suurendada tehnoloogilist jätkusuutlikkust ja tõsta avaliku sektori kuluefektiivsust, sest pilvetehnoloogia lahendused võimaldavad paindlikku ressursikasutust ja tarkvaralitsentsi poliitikat ning lihtsustavad pilveplatvormile loodud rakenduste kasutamist riigiüleselt.

Eelloetletud eesmärkide tausta avatakse lähemalt kontseptisooni esimeses peatükis. Teises peatükis käsitletakse Eesti riigipilve lahendust, kolmandas peatükis selle rakendusplaani ning neljandas kontseptsiooni rakendamise riske koos maandamismeetmetega. Lisaks sisaldab kontseptsioon Eesti riigipilve ja andmesaatkondade rajamise tegevuskava.

Kontseptsiooni on välja töötanud Majandus- ja Kommunikatsiooniministeerium (MKM) Riigi Infosüsteemi Ameti (RIA), Välisministeeriumi (VäM), Rahandusministeeriumi (RaM), Siseministeeriumi (SiM), Justiitsministeeriumi (JuM), Riigi Infokommunikatsiooni Sihtasutuse (RIKS), Andmekaitse Inspektsiooni (AKI), Registrite ja Infosüsteemide Keskuse (RIK), Siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT), Vabariigi Presidendi Kantselei, Rahandusministeeriumi Infotehnoloogiakeskus, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti Infosüsteemide Audiitorühing ning EENet kaasabil.

1. Riikliku IT korralduse ja IT majutusressursside hetkeolukord

2013. aastal analüüsiti Rahandusministeeriumi tellimusel IKT ressursside konsolideerimise vajadust ja võimalusi Eestis.[7] Analüüsi eesmärk oli selgitada välja riigi toimimiseks optimaalne infrastruktuur lähtudes alljärgnevast:

- säilima peab riigi hajutatult paiknev IT arhitektuur s.t iga ministeerium/asutus peab säilitama oma praeguse rolli klientide ja eelarve omanikuna;
- peab säilima võimalus vabaks konkurentsiks;
- ministeeriumite/asutuste IKT-teenuste kvaliteet peab paranema.

Analüüsi lõppraportis rõhutatakse **vajadust konsolideeritud andmesidevõrgu ja** kehtivatele **turvalisusstandarditele vastava andmekeskuse kihi** järele, mis aitaks luua kvaliteetseid ja efektiivseid teenuseid. Käeoleva kontseptsiooni koostamise ajal on andmesidevõrgu konsolideerimine käimas, kuid alustada tuleb ka andmekeskuse kihi konsolideerimisega.
IT majutusressursside konsolideerimine ja Eesti riigipilve loomine lähtub eelkõige vajadusest tagada digitaalne järjepidevus[8] ja tõsta teenuste kvaliteeti.

1.1. Riigiasutuste riistvaralise taristu IT riskid

Eesti riigi infosüsteemi IT arhitektuuri iseloomustab märkimisväärne hajutatus. Riiklike IT küsimustega tegeldakse mitmes institutsioonis. Kuigi riigi tasandil on olemas nii riigiasutuste vahelise andmesidevõrgu teenuse (ASO) kui ka kanali (eesti.ee) kiht, on eelarvete piiratuse ja kompetentse personali vähesuse tõttu asutuseti teenuste kvaliteet ebaühtlane.

See on põhjendatav asjaoluga, et ministeeriumite valitsusalasse jäävate IKT-teenuste korraldamisega tegeleb iga asutus eraldi ning reeglina on selleks asutustes loodud iseseisev IKT-üksus. Sõltuvalt asutuse põhitegevusalast toimub vajalike kompetentside väljaarendamine kas täielikult või osaliselt taolises üksuses, alternatiivina ostetakse need kompetentsid/teenused sisse välistelt teenusepakkujatelt. Asutuste IKT üksustes on üldjuhul vähe töötajaid ning seepärast tuleb töötajal täita mitut erinevat rolli, mistõttu on personaliga seotud riskid kõrged. Ühte ja samasse juhtimisalasse jäävate asutuste vahel puudub ka tihe koostöö, seetõttu esineb palju dubleerimist ning ressursside kasutamine ei ole piisavalt efektiivne.[9]

Samuti puudub käesoleval ajal Eesti avalikul sektoril võimalus oma infosüsteemide majutamiseks kergesti ligipääsetavates ja turvalistes andmekeskustes. Infosüsteemid paiknevad üldjuhul asutuste endi poolt väljaehitatud ja hallatavates, ühte piirkonda koonduvates ruumides, mis aga kõrgelt arenenud Eesti digitaalset ühiskonda silmas pidades ei vasta turvalisuse, energiakasutuse ja ressursside efektiivse kasutamise osas tänapäeva nõuetele.[10] Käesoleval ajal pakub riigiasutustele ja teiste riigieelarvelistele institutsioonidele kõrge kvaliteediga majutust tänapäevastes serveriruumides ainsana RIKS.

---

[7] Martin Noormaa "Riigi IKT analüüsi tulemused." Tallinn, 2013. Analüüsi kokkuvõttev videoesitlus on kättesaadav: https://vimeo.com/65281943.
[8] Digitaalse järjepidevuse peetakse silmas riigi võimekust säilitada riigi toimimise seisukohast olulisi andmeid ja digitaalseid teenuseid sõltumata mistahes muutustest keskkonnas.
[9] Rahandusministeeriumi infotehnoloogia osakond. "Riigi info- ja kommunikatsioonitehnoloogia korralduse analüüs" 2013.
[10] Hinnanguliselt on 60% ruumidest nõuetele mittevastavad.

Eelkirjeldatud fragmenteeritus ja majutusressursside võimalused on IT riskide maandamiseks loonud vajaduse dubleerivate, väljaspool Tallinna paiknevate, turvaliste riiklike andmekeskuste järele, mis vastaksid teenuse (serveriruumid - sealhulgas elekter, ühilduvus, jahutamine ja turvalisus; virtuaalmasinad - sealhulgas serverid kuni operatsioonisüsteemini; mäluseaded; tsoneerimine ja haldus) kokkulepitud tasemele ning mis võimaldaksid luua toimiva riigipilve. Andmekeskuste geograafiline hajutatus on kriitiline teenuste opereerimiseks olukordades, kus mingitele piirkondadele on ligipääs piiratud.

1.2. Eesti riigi julgeoleku ja digitaalse järjepidevuse tagamine

Paberivabale haldusele üleminek on toonud kaasa olukorra, kus üha enam olulist avalikku teavet ja riiklikke registreid eksisteerib ainult digitaalsel kujul – ühe näitena saab tuua Eesti kinnistute andmeid sisaldavat Kinnistusraamatut.[11] Eesti laiapindse riigikaitse arengukavas 2013-2022 ühe julgeoleku ohuna nimetatud muu hulgas ka infoühiskonna haavatavused.[12] Riigi vastu suunatud ja läbimõeldud küberintsident võib kaasa tuua soovimatuid tagajärgi kogu ühiskonnale. Seetõttu on digitaliseerimisega arvestamine muutunud möödapääsmatuks ka riigikaitses ning küberturvalisuse tagamine on julgeoleku suundades määrava tähtsusega.

Seni ei ole küberrünnakud riigile küll märkimisväärset materiaalset kahju põhjustanud, kuivõrd üldjuhul on rünnatud avalikke veebisaite, mis ei kuulu riigi jaoks kriitilise tähtsusega infrastruktuuri hulka. Seega ei ole ajutised tõrked selliste veebisaitide töös ohustanud inimelusid ega Eesti riigi toimimist tervikuna. Teisalt on erandiks sümboolse staatusega veebisaidid ehk nn „monumendid" (näiteks Kaitseministeeriumi, Presidendi jmt veebilehed), mida peab kaitsma kahjustamise või näotustamise[13] eest iga küberkaitset oluliseks pidav riik. Väikseimgi tulemuslik rünnak kahjustab selle ohvriks langenud riigi mainet, vähendab usaldusväärsust ning võib põhjustada ühiskonnas segadust.

Eesti digitaalse järjepidevuse tagamine kujutab endast palju enamat kui seda on kriitilise tähtsusega andmehulkade ja IT-lahenduste alalhoidmine Eesti territooriumil - nimelt tuleb leida lahendused ka olukordadeks, kus Eesti riigil puudub kontroll tema enda territooriumil paiknevate andmekeskuste üle. Lisaks võib tekkida vajadus osade teenuste osutamiseks väljaspool Eesti riigi piire.

Peamine väljakutse seisneb siin sellise lahenduse väljatöötamises, mis tagaks avalike teenuste toimimise eelkirjeldatud olukordades. Mitteavaliku sisuga ja isikuandmetega (sh. delikaatsete isikuandmetega) infosüsteemide puhul lisandub täiendava keerukusena andmete terviklikkuse ja puutumatuse tagamise vajadus. Sellise lahenduse realiseerimine on ka üks küberjulgeoleku strateegia eesmärke.[14]

1.3. E-riigi areng ja piirideta riik

Eesti ühiskond sõltub olulisel määral IKTst. Asjaajamine ja tehingute tegemine elektroonilise isikutunnistusega on kujunenud igapäevaseks ja iseenesest mõistetavaks praktikaks. Alates 2014. aasta 1. detsembrist väljastab Eesti ka mitteresidentidele digitaalseid isikutunnistusi.[15] Üleilmset tähelepanu

[11] https://kinnistusraamat.rik.ee/detailparing/Login.aspx?ReturnUrl=%2fdetailparing%2f.
[12] Kaitseministeerium "Riigikaitse arengukava 2013-2022 mittesõjalised osad." Kättesaadav: http://kra.ee/static/riigikaitse_arengukava_2013_20221.pdf.
[13] Näotustamine on veebisaidi ametliku sisu rikkumine
[14] „Küberjulgeoleku strateegia 2014 – 2017". Avalik versioon on kättesaadav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
[15] https://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/e-residendi-digi-id/.

pälvinud e-residentsuse kontseptsioon loob ainulaadse võimaluse distantsilt kasutatavate globaalsete teenusegruppide väljatöötamiseks ning võimaldab pakkuda täiesti uudseid avaliku- ja erasektori teenuseid – pangatehingud, maksuaruandlust, meditsiinilist nõustamist jne - sõltumata nende kasutaja asukohast.[16]

Riik plaanib sel moel luua tugeva aluse uute ärivõimaluste tekkeks. Selleks vajaliku infrastruktuuri ja teenusevaliku väljaarendamine nõuab aga avaliku- ja erasektori ühiseid jõupingutusi ja tegevuste omavahelist kooskõlastamist. E-residentsuse leviku ja edu saavutamiseks on vajalik tagada digitaalne järjepidevus ning riiklikke registrite, millega on seotud isikute omandistaatus, säilivus. Näiteks tuleb välistada olukorrad, kus e-resident kaotaks mingil põhjusel oma maaomandi. Seega on e-residentsuse projekti edu tagamiseks vajalikud teatud garantiid (näiteks tagada omandilise kuuluvuse tõestamiseks digitaalne järjepidevus, mis seonduvad eeskätt Äriregistri ja Kinnistusraamatu teenustega).

E-residentsuse kasutuselevõtt sunnib Eestit tooma oma avaliku- ja erasektori teenused klientidele lähemale, mis omakorda suurendab vajadust pilvandmetöötluse võimaluste väljaarendamiseks nii Eesti riigi piires kui ka väljaspool seda.

1.4. Infosüsteemide turvameetmete rakendamine

Riigi ja kohalike omavalitsuste infosüsteemides, neis oleva teabe ja andmete turvalisuse tagamiseks on kohustus rakendada ISKEt.[17] Aastal 2013 vastas ISKE nõuetele RIA läbiviidud analüüsi põhjal ca 40% riigiasutuste ja kohaliku omavalitsuse serveriruumidest.[18]

Konkreetsemateks probleemideks olid infosüsteemide majutamiseks kasutatavad nõuetele mittevastavate ruumid, nendes kliimaseadmete puudumine, ruumide ebapiisav füüsiline turve ja ebakorrapärane seadmestiku hooldus.

IKT taristule kohalduvate ISKE turvameetmete rakendamise tõhustamiseks on riigil mõistlik pakkuda keskselt turvalist ja kvaliteetset IKT taristut.

1.5. Kulu-efektiivsus ja tehnoloogilise jätkusuutlikkuse tagamine

Kulude säästmise vajadus sunnib avaliku halduse asutusi oma tööprotsesse optimeerima ja otsima igapäevasteks töövahenditeks (mh nt e-post, failihaldus, tootlikkuse tarkvara jne) paindlikke lahendusi ning ökonoomsemaid litsentsitingimusi. Eestis on üle 200 omavalitsusüksuse ning kuna nad vastutavad maade planeerimise, sõiduteede korrashoiu, sotsiaal-, haridus- ja muude paljude kohaliku tasandi avalike teenuste pakkumise eest, siis on efektiivse kontoritarkvaralahenduste leidmine äärmiselt keeruline. Seetõttu on mõistlik erinevate teenuste pakkumiseks loodud rakendusi kasutada riigiüleselt ning pilvetehnoloogia pakub selleks sobivat võimalusi SaaS[19] teenuse näol. Selline lahendus toetab innovatsiooni ning tagab infosüsteemide ajakohasuse ja tehnoloogilise järjepidevuse. Lisaks ei ole enam vaja osta litsentsi igale töökohale eraldi, kuna hinnakiri sõltub toote tegelikust kasutamisest.

[16] Siseministeerium „Uus digilahendus annab välismaalastele võimaluse e-Eestis tegutseda" Tallinn, 2014.
[17] www.ria.ee/iske,VV määrus „Infosüsteemide turvameetmete süsteem", kättesaadav: https://www.riigiteataja.ee/akt/13125331?leiaKehtiv.
[18] Riigi Infosüsteemi Amet „Eesti riigiasutuste ja ETO-de serverimajutuse võimekus" 2013.
[19] SaaS (*Software as a Service*) tarkvara teenusena, kus asutus ei pea endale ise tarkvara litsentsi ostma ja installeerima, vaid saab kasutada pilves olevat rakendust. See võimaldab asutustel jagada arendatud rakendusi (nt dokumendihaldussüsteemid, ressursside planeerimine, e-post, jt).

Riigipilve kasutamisel ei pea iga riigiasutus endale enam hankima serverimajutuse riistvara (sealjuures veel arvestama teatud võimsusvaruga) ja seda kahte erinevasse lokatsiooni paigaldama, vaid selle eest hoolitseb riigipilveteenuse operaator, kes optimeerib riigiasutuste ressursside kasutuse ning hoolitseb ka serverimajutuse erinevate lokatsioonide eest. Konsolideerimine ja mastaabi-efekt võimaldavad vähendada serverimajutusele kulutatavaid summasid. Kokkuhoid tekib kui riigipilv on edukalt tööle rakendunud ning on tekkinud piisav hulk riigipilve kasutajaid.

2. Lahendused Eesti riigipilve rajamiseks

Eesti riigipilve lahenduseks on hübriidpilv,[20] mis koosneb kolmest komponendist:

1) Eesti riigi privaatpilv;[21]
2) avalike pilvede[22] kasutamine;
3) andmesaatkondade võrgustik.

Eelnimetatud kolm osa moodustavad Eesti riigipilve terviklahenduse. Esimeseks sammuks riigipilve loomisel on riigi privaatpilve rajamine ning tänaste riiklike infosüsteemide arendamine selliselt, et need oleks võimelised pilvetaristu omadusi kasutama (nt infosüsteem peab olema võimeline ühest lokatsioonist teisele lülituma, automaatselt üles ja alla skaleeruma jms). Käesoleval ajal ei ole riiklikud infosüsteemid võimelised täiel määral pilvetehnoloogia omadusi kasutama, mistõttu on infosüsteemide kaasajastamine oluline, et tekitada võimekus nende opereerimiseks andmesaatkonnast või avalikust pilvest.

2.1. Eesti riigi privaatpilv

Eesti riigi privaatpilve üks peamine eesmärk on **asutuste IT ja turvariskide maandamine**, kuivõrd see võimaldab asutustel oma infosüsteemid paigutada turvalistesse ja standarditele vastavatesse majutuskeskkondadesse. Samuti lihtsustab lahendus asutuste auditeerimiskohustust, sest riigipilv võimaldab nõuetekohase auditeerimise selle alumistele kihtidele (serveriruumid, võrguseadmed, serverid, kettakastid).

Teiseks privaatpilv **suurendab digitaalset järjepidevust,** sest infosüsteemide migreerimine pilveplatvormile toob vajaduse kaasajastada infosüsteemid vastavuses infosüsteemide opereerimise alusnõuetega pilves. Eesti riigi privaatpilve rajamisega **luuakse eeldused infosüsteemide opereerimiseks andmesaatkondadest** või **avalikest pilvedest,** kui vastav vajadus tekib. Samuti e-teenuste käideldavus pilveplatvormi kasutamisel suureneb, kuid seda eeldusel, et asutuste infosüsteeme kaasajastatakse ja disainitakse ümber pilvetehnoloogia võimalusi kasutama.

Kolmandaks **võimaldab riigi privaatpilv riigi IT ressursse efektiivsemalt kasutada ja suurendab haldussuutlikkust,** sest andmekogude majutus- ja haldusteenuse eest hoolitsevad valdkonna parimad spetsialistid ning väheneb kompetentside, riistvara ja ka tarkvara dubleerimine. Pilveteenuseid hinnastatakse vastavalt ressursside reaalsele kasutusele, mis võimaldab vajadusel arvutusressurssi ja

[20] Hübriidpilv on kombinatsioon kahest või enamast pilvest (privaatpilv, kommuunpilv ja avalik pilv), mis jäävad ainulaadseteks üksusteks, kuid on siiski omavahel kokku seotud, pakkudes eri pilvandmetöötluse mudelite kõiki boonuseid. Näiteks võimaldades hoida tundlikke andmeid organisatsiooni privaatpilves ja avalike andmeid avalikus pilves.
[21] Privaatpilv on pilvekeskkond, mis on eraldatud ainult ühe organisatsiooni jaoks.
[22] Avalik pilv on pilvekeskkond, mille ressursse ja rakendusi saab iga soovija kasutada.

andmemahtusid kiirelt juurde tekitada ning seeläbi suureneb kuluefektiivsus ja ressursikasutuse paindlikkus. Samuti võimaldab lahendus kasutusele võtta pilvetehnoloogia PaaS[23] ja SaaS platvormid, mis võimaldavad **ühtlustada asutustes kasutatavaid IT lahendusi ning toetavad e-teenuste innovatsiooni**. Lisaks koonduvad kokku ühte asutusse valdkonnas pädevad inimesed ning seeläbi kaob riigiasutuste vaheline konkurents vastava kompetentsiga personali pärast, mistõttu muutub lihtsamaks uute inimeste värbamine ning ka järelkasvu koolitamine.

Eesti riigi privaatpilve keskmes on klassikaline andmekeskuse lahendus, mis erineb väga vähe teistest mujal maailmas kasutatavatest riigipilve mudelitest. Peamine erinevus on tingitud Eesti väiksusest, mis muudab konkurentsi tekkimise keeruliseks ja suuremahulistest hangetest saadava kulude kokkuhoiu minimaalseks. Avalik sektor, välja arvatud munitsipaalasutused, vajab 2013. aastal läbi viidud RIA uuringu põhjal andmekeskuse jaoks ruume kogupindalaga umbes 2000 ruutmeetrit.[24] Turvalisuse kaalutlustel vajab Eesti ka teist sellist asukohta (sekundaarset andmekeskust), mistõttu on koguvajadus vähemalt 3000 m^2 pinna järele. Nende hinnangute juures on arvestatud ka andmemahtude kasvuga. Sekundaarse andmekeskuse pinnana on võimalik kasutada juba olemasolevaid ISKE nõuetele vastavaid ruume, mille peamiseks opereerijaks on RIKS. Nõuetele vastava privaatpilve[25] rajamiseks ja riigiasutuste serverimajutuse konsolideerimiseks on vaja ehitada riigi primaarne andmekeskus, mis võimaldaks infosüsteemide paigutamist kvaliteetselt, turvaliselt ja hajutatult erinevatesse lokatsioonidesse.

Uus andmekeskus võimaldab lahenduse järgmistele probleemidele:

a) aitab täita riigipilvele esitavaid nõudeid[26] (nt riigipilve teenuse käitamine minimaalselt kahes erinevas füüsilises asukohas, mis vastavad turvastandardi ISKE klassile H+);

b) lahendab riigiasutuste serverimajutusressurssi puuduse ja selle kvaliteedi probleemi (võimaldades kasutada nõuetele vastavaid serveriruume ka nendele asutustele, mis ei soovi riigipilvega liituda);

c) toetab laiapõhjalist riigikaitset (hetkel on kõik andmekeskused koondunud Tallinna piirkonda, kuid uus andmekeskus asuks Tallinna piirkonnast väljas ja see võimaldab asutustel majutada oma andmeid hajusamalt);

d) võimaldab energia- ja keskkonnasäästlikumat serverimajutust kui senised lahendused.

Riigi uue andmekeskuse ehitamine lahendaks asutuste serverimajutuse probleemi keskselt. RIA läbiviidud küsitluste põhjal ja RIA baasinfrastruktuuri nõukogus on selgunud, et lähiaastatel on mitmetel riigiasutustel vaja oma andmekeskusi uuendada või uued rajada.

Omaette küsimus puudutab asutuste erinevat ressursside kasutust andmesidevõrguga ühinemiseks ja tulemüüri kasutamist privaatpilves. Selleks tuleb luua turvaklassid, mille alusel määratletakse avalikus

[23] PaaS (*Platform as a Service*) platvorm teenusena, kus kasutajale võimaldatakse lisaks pilve infrastruktuurile ka operatsioonisüsteem ja andmetöötlusplatvorm (nt PaaS pakub ka andmebaase ja veebiservereid).
[24] RIA „Riiklikke andmekeskuste konsolideerimine ja ehitamine".
[25] RIA „Nõuded riigipilvele", kättesaadav: https://www.ria.ee/riigiarhitektuur/wiki/lib/exe/fetch.php?media=an:riigipilve_alusnouded.pdf
[26] RIA „Nõuded riigipilvele", kättesaadav: https://www.ria.ee/riigiarhitektuur/wiki/lib/exe/fetch.php?media=an:riigipilve_alusnouded.pdf.

IP-ruumis või spetsiifilises võrgutsoonis paiknevad riigipilve osad. Andmekeskused ja asutused peavad olema omavahel ühendatud informatsiooni turvalise edastuskanalite kaudu.

2.2. Avaliku pilve kasutamine

Pilvandmetöötluse ressursside haldamine peab toimuma võimalikult paindlikult. Isegi Eesti-suuruses väikeriigis esineb tippnõudlusega perioode (nt elektroonilise tuludeklaratsiooni täitmise ajal). Seega tuleb Eesti riigipilve lahendusse kaasata ka erasektori võimalused, et **suurendada ressursside kasutamise efektiivsust.** Avalike andmete paigutamisel avalikesse pilvedesse on need ka kodanikele lihtsamalt kättesaadavad.

Eesti on kasutanud rahvusvaheliste suurkorporatsioonide pilveteenuseid 2009. aastast alates, mil riiklik turismisait visitEstonia.com koliti Amazoni pilve. Pilvemajutuse kasutamine oli toona tingitud eeskätt vajadusest paindliku serveriressursi halduse järele. Lisaks koormustaluvusele vajas klient (EAS) ennekõike piisavat talitlusvõimet, mis omakorda tähendas portaali toomist selle peamisele sihtrühmale lähemale. See sai võimalikuks tänu rahvusvahelise avaliku pilve lahenduste kasutamisele.

Eestis on pilvetarkvara võimalik kasutada e-posti, koostöögruppide, failihalduse jms eesmärkidel isegi siis, kui pilv ise paikneb väljaspool Eesti territooriumi. Andmekaitse Inspektsioon ei näe pilveteenuste kasutamises ja informatsiooni liikumises väljapoole Eesti riigi piire põhimõttelisi takistusi seni, kuni töödeldavad andmed ei ole isikuandmed sh delikaatsed isikuandmed või muude avaliku teabe seadusest tulenevate piirangutega seotud. Eesti seadusandlusest tulenevalt ei ole erisust, kas teenust osutatakse Eestis või väljaspool seda, eeldusel, et andmeid töödeldakse andmekaitse direktiivist[27] ja isikuandmete kaitse seadusest[28] lähtuvalt. Sellele vaatamata tuleks avalike pilvelahenduste korral neisse informatsiooni ja andmete viimise lubatavust koostöös Andmekaitse Inspektsiooniga analüüsida ja hinnata. Näiteks omavalitsuste tasandil saaks pilveteenuste abil saab oma teenuste kvaliteeti tõsta, sest enamus seal kasutatavaid andmeid on juurdepääsu piiranguta ja avalikud (juurdepääsupiiranguga andmete hulka kuuluvad peamiselt erinevad toetused ja load, isikuandmed ning hangetega seotud informatsioon). Juurdepääsupiiranguga andmete hoidmist avalikes pilvedes, ka krüpteeritud kujul, tuleb kindlasti hoolikalt kaaluda ning vajadusel piirata andmete lekkimisega kaasneda võiva kahju tõttu. .

Teisalt võib avalike pilveteenuste kasutamine juurdepääsupiiranguga andmete hoidmiseks tulla varuvariandina kõne alla kriisi- või sõjaolukorras, kus **vajadus digitaalse järjepidevuse säilitamise järele** kaalub üles ebatõenäolised juurdepääsupiirangutega andmete lekkimisega kaasnevad riskid. Samuti tasub mõelda kriitilise tähtsusega (näiteks Riigikogu või Vabariigi Valitsuse) teenuste opereerimisele väljaspool Eesti territooriumi paiknevatest avalikest pilvedest kriisiolukorras. Lisaks nende rakenduste poolt tagatud informatsiooni kaitsmisele on turvalisuse suurendamiseks võimalik kasutada Eesti riigi baasinfrastruktuuri pakutavat krüpteerimise võimekust. Kodanike andmete kaitsmine on keskne teema riigipilve väljaarendamisel ja mistahes avalikke pilvede kasutamisel.

[27] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ „Üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vabaliikumise kohta.“ Kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:ET:PDF.
[28] Isikuandmete kaitse seadus, kättesaadav: https://www.riigiteataja.ee/akt/112072014051?leiaKehtiv.

Avalike pilvede kasutamine **aitab lahendada ka litsentside ja tarkvara soetamisega seotud küsimusi**. Seega on igati põhjendatud arvestada rahvusvaheliste korporatsioonide pakutavate teenusemudelitega nagu IaaS[29], PaaS ja SaaS ka riigipilve arhitektuuris.

Rahvusvaheliste pilveteenuste pakkujate hinnakiri ja teenuste kvaliteet on sobivad nn „monumentide" (näiteks President.ee, Valitsus.ee) kaitsmise seisukohast. Riigi mainega seotud veebisaitidele suunatud võimalike rünnakute ärahoidmiseks on mõistlik tellida kaitselahendused väljastpoolt Eestit ning kasutada taoliste veebisaitide majutamiseks rahvusvahelist avalikku pilve. Need veebisaidid ei sisalda tundlikku informatsiooni ning serverifarmid ja informatsiooni hajutatus muudavad nende ründamise ebamõistlikult kulukaks. Ehkki avalike pilvede kasutamine kätkeb endas teatud riske, kuivõrd need ei pruugi olla täielikult kättesaadavad, pakuvad nad üldjuhul siiski **suuremat võimekust tulla toime enamlevinud teenustõkestuse rünnakutega**[30] võrreldes ministeeriumite ja asutuste vastavate oskuste ja võimalustega käesoleval ajal. Samuti on avalikus pilves serveriressursside administreerimine väga lihtne. Vajadusel saab paari nupule vajutusega serveriressurssi juurde hankida või seda vähendada. **See võimaldab asutustel kasutada majutusressursse vajaduspõhiselt ning oma arvutusvõimsused kuluefektiivselt optimeerida.**

Eesti kasutab juba mitmeid avaliku pilve teenuseid (nt Offiice 365, visitEstonia.com'i majutamine AWS-is jt). Seetõttu on oluline kaasata avalike pilveteenuste pakkujad Eesti riigipilve kontseptsiooni. Samas, kuna riigil puudub selliste andmete hoidmise ja asukoha üle täielik kontroll, tuleb alati arvestada andmete lekkimise võimalusega.

2.3. Andmesaatkondade rajamine

Digitaalse järjepidevuse hoidmine ja e-residentidele täiendavate garantiide andmine on teemad, mis annavad pilveteenuste kasutamise osas selget tunnistust Eesti spetsiifikast võrreldes teiste riikide vajadustega. Eesti vajab täiendavat serveriressurssi, mis oleks küll täies ulatuses Eesti Vabariigi kontrolli all, kuid paikneks väljaspool Eesti territooriumi. Oluliste andmete ja rakenduste varundamisel järgitakse juba praegu kindlaid protseduurireegleid, millest kinnipidamine võimaldab teenuse tänu varukoopiate olemasolule vajadusel taastada.

Digitaalse järjepidevuse tagamiseks on mõnedest registritest (nt kõiki Eesti õigusakte koondav võrguväljaanne Riigi Teataja) siiski vaja selliseid aktiivseid koopiaid, mis on kasutatavad reaalajas ja mida saab seadusest tulenevalt uuendada ka olukordades, kus Eesti riigil puudub kontroll Eesti territooriumil paiknevate andmekeskuste üle või kus tegemist on mõne muu kriisi- või hädaolukorraga, mis muudab Riigi Teataja rakenduse Eestist opereerimise võimatuks. Kriitilisteks andmekogudeks on määratletud Riigikassa infosüsteem, Riigi Teataja, Kinnistusraamat, Äriregister, e-toimik, Rahvastikuregister, Pensionikindlustuse register, Maksekohuslaste register ning Isikut tõendavate dokumentide register.[31]

[29] IaaS (*Infrastructure as a Service*) on pilve infrastruktuuriteenus, kus kliendile võimaldatakse taristu - serverid, võrgundus, salvestusruum, jt.
[30] Üks järeldus, mis tekkis MKMi ja Microsofti ühises uurimusprojektis „Implemenatation of Virtual Data Embassy Solution." Kättesaadav: https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf .
[31] RIA andmekogude töörühma seisukohast (AK-märkega dokument).

Seda loetelu tuleb perioodiliselt üle vaadata ja vajadusel täiendada, kuid oluline on selliseid **riiklikult kriitilisi andmekogusid turvaliselt, regulaarselt ning kindlate reeglite järgi varundada**. Sellise ressursi tagamiseks kavandatakse valikuliselt sõbralike välisriikide Eesti saatkondadesse rajada serveriruumid ehk **andmesaatkonnad.** Vajalike tehnoloogiliste ressursside olemasolul saab andmesaatkondi kasutada registrite varukoopiate hoidmiseks. Suurematesse saatkondadesse saab luua spetsiaalseid keskkondi, kus toimub regulaarne andmete ja rakenduste varundamine, teenuste peegeldamine ja vajadusel opereerimine. **Andmesaatkonnad on riigi privaatpilve laiendus Eesti riigi territoriaalsetest piiridest väljapoole.** Sellisele mudelile üleminek ja andmete iganädalane varundamine annaks Eestile võrreldes praegusega märkimisväärse eelise, kuna praegune, kord kvartalis või kaks korda aastas toimuv varundamine ei võimalda andmeid piisavalt tihti uuendada ega seetõttu digitaalset järjepidevust täielikult kindlustada.

Samas kaasnevad Eesti saatkondade kasutamisega ka teatud probleemid. Nimelt jääb saatkondadel vajaka tehnilisest kompetentsist, mis tagaks infrastruktuuri alalhoidmiseks ja kriisiolukorras reageerimiseks vajalikul tasemel tehnilise võimekuse. Teiseks puudub saatkondadel kontroll neile pakutava telekommunikatsiooniteenuse üle. Seetõttu võib juhtuda, et küberintsidendi käigus blokeeritakse rünnatav võrgusegment eesmärgiga vältida teiste sama võrgu ressursside ülekoormust ning seeläbi katkeb andmesaatkonna ühendus riigipilvega.

Selliste olukordadega tegelemiseks võib tulevikus kaaluda kahepoolsete kokkulepete alusel ressursside hankimist Eestiga sõbralikes suhetes olevate riikide andmekeskustest. Sellisel juhul rendiks Eesti sõbraliku riigi andmekeskuses vajalikku põrandapinda või eraldatud ruumi, mis vastab nõutud standarditele. Sellise ruumi perimeeter oleks ümbritsevast alast füüsiliselt eraldatud ja varustatud turvaseadmetega, tagamaks Eesti riigi täieliku kontrolli vastavasse perimeetrisse jääval alal paiknevate serverite üle. Sarnaselt füüsilistele saatkondadele kuuluks ka selline kindlaksmääratud perimeetris paiknev ala Eesti jurisdiktsiooni alla ning sellele kohaldataks samasuguseid sätteid (kaasa arvatud immuniteet) nagu füüsilistele saatkondadele või suursaadikute residentsidele. Selline lahendus täiendaks oluliselt Eesti riigipilve lahendust, sest Eestiga sõbralikes suhetes oleva riigi andmekeskused on rajatud spetsiaalselt andmete talletamiseks, kus erinevate riskide (ülekuumenemine, voolukatkestused, võrgu ülekoormus, kaablite kahjustumine jne) esinemise tõenäosus on viidud miinimumini. Spetsiaalselt rajatud andmekeskustes kehtivad teenuste kvaliteedi osas spetsiifilised nõuded ja neis töötab professionaalne meeskond, kes on saanud väljaõppe küberrünnakute tõrjumiseks ja teenuste kättesaadavuse tagamiseks kriisiolukorras.

Eesti saatkondades paiknevad serveriruumid moodustaksid digitaalse järjepidevuse tagamiseks vajaliku võrgustiku, mille kahjustamine või rivist väljalöömine oleks potentsiaalse vaenlase jaoks keeruline ja kulukas ettevõtmine. Tulevikus võib täiendavalt kaaluda andmesaatkondade rajamist ka Eestile sõbraliku riigi andmekeskustesse.

Tuleb kindlasti arvestada, et kõik andmesaatkonnad on teiste saatkondadega interneti kaudu ühendatud ning andmevahetus toimub krüpteeritud kujul.

2.4. Kokkuvõte Eesti riigipilve lahendusest

Kokkuvõtteks võib öelda, et Eesti riigipilve kontseptuaalses mudelis on esindatud kolm omavahel põimuvat kihti:

1) Eesti privaatpilv, mille eelduseks on nõuetele vastavate riigi primaarse andmekeskuse rajamine ja olemasolevate riigi andmekeskuste ühendamine;

2) avalikke pilvede teenuste kasutamine, kuid mille kasutamisel on arvestatud, et seal hoitav informatsioon on nõuete kohaselt kaitstud;

3) andmesaatkondade võrgustik, mis on Eesti privaatpilve laiendus Eesti riigi territoriaalsetest piiridest väljapoole. Võrgustikku kuuluvad Eesti füüsilistesse saatkondadesse rajatud serveriruumid.

Riigipilve keskseks osaks on privaatpilv, mis loob eeldused avalikke pilvede ja andmesaatkondade ühendamiseks terviklikuks ja funktsionaalseks riigipilveks. Riigipilve osad on ühendatud informatsiooni edastusese kanalitega, mis on vajadusel krüpteeritud, et tagada turvaline internetipõhine andmevahetus avaliku- ja erasektori ettevõtete vahel.

Põimuvate kihtide kombineerimisel tekib Eesti riigipilv, mis vastab vajalikele nõuetele ning ühtlasi võtab arvesse Eesti spetsiifilisi väljakutseid: tagada digitaalne järjepidevus ja usaldusväärsed e-teenused nii Eesti riigi kodanikele kui ka e-residentidele, riigiasutuste IT riskide ja IT korralduse fragmenteerituse vähendamine, teenuste kvaliteedi tõstmine ning efektiivsete ja innovaatiliste pilvetehnoloogia lahenduste kasutuselevõtminekogu avalikus halduses.

3. Eesti riigipilve rakendusplaan

3.1. Eesti riigi privaatpilve ehitamine

Eesti privaatpilve ehitamisel on esmajoones tarvis **luua toimiv baastaristu**, millele riigi privaatpilv rajada. Selleks on esmalt vaja kokku leppida **riigi primaarse andmekeskuse ehitamises,** mis vastaks ISKE H+ tasemele.[32] Välja tuleb valida nõuetele sobilik asukoht, sätestada tehnilised tingimused ja andmekeskuse optimaalne suurus. Andmekeskuse ehitamise, projekteerimise ja opereerimise eest vastutab RIKS ning selle asukoht kooskõlastatakse küberjulgeoleku nõukogus. Andmekeskuse valmimisel 2018. aastal saavutab riigi privaatpilv oma täisfunktsionaalsuse.

Riigisiseste serveriressursside konsolideerimine tuleb lõpule viia ning rakendada **serveriressursside haldamiseks ja arendamiseks ettenähtud ärimudelit**. Konsolideerimise protsess toimub järkjärgult, sest asutuste serverimajutuse tingimused on erinevad ning seetõttu liituvad asutused riigipilvega erinevatel ajahetkedel, vastavalt serverimajutuse vajaduse tekkimisele. Edaspidi peavad ministeeriumid ja asutused oma serveriressurssidega vajadustega pöörduma RIKSi poole, mis vastutab andmete majutus- ja haldusteenuste osutamise eest riigiasutustele. RIKS võimaldab vajalikud vahendid arendavatest majutusressurssidest (pakkudes vastavalt asutuse soovile kas riigipilve või serveriruumi rendi teenust) või hangib võimekust juurde erasektorist. RIKSi arengukavast[33] lähtuvalt kasutatakse serverimajutuse üksuste

[32] RIA „Andmekeskuste turvanõuded“, kättesaadav: https://www.ria.ee/public/KIIK/AndmekeskuseTurvanouded.pdf.
[33] RIKSi arengukava aastateks 2015 – 2019., kättesaadav: http://riks.ee/images/659.pdf .

lõplikul väljaarendamisel juba olemasolevaid üksusi ning juurde rajatakse riigi primaarne andmekeskus. Riigi privaatpilve lahenduse piloteerimiseks saab kasutada olemasolevaid andmekeskusi, kuid nõuetele vastava riigi privaatpilve jaoks on vaja ehitada juurde riiklik andmekeskus.

RIKS on välja töötanud **uue andmekeskuste esialgse rakendusplaani** ja alustanud läbirääkimisi erasektori ettevõtetega, kellele juba kuulub Eesti territooriumil RIA kehtestatud standarditele vastavaid andmekeskusi ja serveriressursse. Eesmärk on vastavalt riigihanke põhimõtetele töötada välja mudel erasektori ressursside paindlikuks kaasamiseks seal, kus see ISKE nõuete kohaselt võimalik on. Riigi privaatpilve rajamiseks, pilveteenuste pakkumiseks ja võimekuse parandamiseks on RIKS palganud tööle pilvelahenduste spetsialistid ja arhitektid.

Täpsustada tuleb pilveteenuse kliendi (ministeeriumid ja riigiasutused) ning müüja (RIKS) vastutuse ulatust. Selleks on RIA kokku kutsunud ekspertide töörühma, kes on välja töötanud nõuded riigi privaatpilve tehniliseks teostamiseks ja rakendamiseks. Üleminek pilveteenustele viiakse ellu kahes etapis, et see oleks kliendile võimalikult sujuv ja mugav. Esimeses etapis vastutab iga pilveteenuse kasutaja operatsioonisüsteemist ise oma IT-lahenduste toimimise ja varundamise eest ning riigipilve teenuste müüja vastutab peamiselt infrastruktuuriga seotud teenuse eest. Esimest etappi tuleb käsitleda sissejuhatava pilootetapina, mis liigub edasi rohkem teenusele orienteeritud mudeli rakendumiseni.

Teises etapis rakendub riigi privaatpilvega seotud terviklik teenusteportfell, millega luuakse riigi IT keskuste ja erasektori jaoks võimalus teha omavahel koostööd, et pakkuda riigi privaatpilve kasutavatele asutustele keerukamaid ja leidlikumaid lahendusi (nt andmebaasi haldus, operatsioonisüsteemi massiline juurutamine, seireteenused, logide kogumine ja töötlemine, spetsiifiliste rakendusserverite ja infosüsteemide haldamine tervikuna). Ettevalmistused selleks etapiks peavad algama samaaegselt esimese etapi elluviimisega. Riigi privaatpilve rajamine toimub etapiviisiliselt ning seetõttu on oluline **töötada välja meetodid riigi privaatpilve seiramiseks, testimiseks, skaleerimiseks ja toimepidevuse tagamiseks**.

Selleks, et riiklikud infosüsteemid oleksid pilves opereerimisvõimelised ja suudaksid kasutada pilvetehnoloogia võimalusi (skaleeruvus, paindlikkus, asukohast sõltumatus jne) **tuleb infosüsteemid vastavalt arendada.** Vastav täiendus tuleb sisse kirjutada riigi infosüsteemi arhitektuuriga sobiva tarkvara tellimise juhendisse[34]. Samuti loob RIA Arhitektuurinõukogu etalonarhitektuuri dokumendi, mis kirjeldab pilvekõlbuliku infosüsteemi põhimõtteid.

Ministeeriumite ja asutuste pakutava ebaühtlase teenuste kvaliteedi tõttu on arutatud täiendavate regulatsioonide vastuvõtmist eesmärgiga kiirendada ühtse riigipilve konsolideerimise protsessi. Selleks on enne **vaja läbi viia kehtiva õiguse analüüs ning vajadusel välja töötada regulatsioonid erijuhtumite tarbeks**, mille alusel ministeeriumid ja asutused võivad omada isiklikku serveriressurssi. Kõigil muudel juhtudel tuleb kasutada RIKSi pakutavaid teenuseid ja rakendada serveriressursi konsolideerimist.

[34] Riigi Infosüsteemi Arhitektuurinõukogu „Tarkvara tellimise juhend“, kättesaadav: https://www.ria.ee/riigiarhitektuur/wiki/doku.php?id=an:soovitused

3.2. Privaatpilve finantseerimine ja riigipilve teenuse eest maksmine

Riigisiseste serveriressursside konsolideerimisel ja riigi privaatpilve loomisel on kandev roll RIKSil, mille põhikiri[35] näeb ette riigiasutustele andmete majutus- ja haldusteenuse osutamist. Arendusprojektid (dubleeriva andmekeskuse ehitamine, riigi privaatpilve rajamine, pilootide läbiviimine) rahastatakse EL struktuurivahenditest. Struktuurivahenditest[36] toetatakse ka riigiasutuste majutusressursside kolimist riigipilve, mis on samuti arvestatav kulu.

Osutatava riigipilve teenuse eest küsib RIKS riigiasutustelt kulupõhist teenustasu. Teenusetasu sisaldab riigipilve opereerimise kulusid kui ka riigipilve amortisatsioonikulusid. Amortisatsioonikulud peavad tagama riigipilve lahenduse jätkusuutlikkuse ja riigipilve taristu uuendamise. Kuna riigiasutused liituvad riigipilvega erinevatel ajahetkedel, sõltuvalt nende olemasoleva taristu seisukorrast, siis lõplik riigipilve teenusehind kujuneb välja, kui riigipilvel on kriitiline hulk kliente ning välja on arendatud riigipilve teenuste pakett. Kuni selle hetkeni on riigipilve opereerimisekulud vaja katta riigi eelarvest, kui riigipilv saavutab täisfunktsionaalsuse, siis hakkavad teenuse eest maksma riigipilve kliendid.

Riigipilve kolimise siirdeprotsessi käigus võivad riigiasutuste halduskulud serverimajutusele küll tõusta, kuid konsolideerimise käigus riigi kulutused andmete majutusele suures plaanis vähenevad (Euroopa Komisjoni hinnangul vähenevad kulutused seeläbi kuni 20%[37]).

Riigi privaatpilve rajamisega kaasneb riigiasutuste eelarvesse oluline muudatus - nimelt **peavad asutused hakkama maksma IT majutusteenuse eest eraldi**, mistõttu nende kulueelarved suurenevad. Praeguseni hankis enamik asutusi majutusressurssi endale läbi asutuse IT investeeringute ning haldas servereid ise, mistõttu eelarvetes eraldi kulurida IT serverimajutusele ei eksisteerinud, vaid see on peidetud teiste kulude sisse. **Nüüd tekib riigipilve klientidele juurde kulurida pilveteenuse kasutamise eest ning asutustele selge ülevaade infosüsteemide ja andme mahtude suurusest.**

3.3. Avalike pilvede kasutamise põhimõtted

Eesti digitaalse järjepidevuse tagamiseks testitakse rahvusvaheliste avalikke pilvede kasutamist. Samal eesmärgil viidi ellu **pilootprojekt, mille käigus katsetati Eesti sümboolse veebisaidi president.ee ja võrguväljaande Riigi Teataja majutamist rahvusvahelises avalikus pilves**.[38] Pilootprojekti tulemusel tekkis teadmus, kuidas veebisaitide toimimist ja veebiteenuseid saab avalike pilveteenuste abil parandada.

RIA juhtimisel analüüsitakse pilvetehnoloogiate turvalise kasutamise põhimõtteid ja luuakse vastavad juhiseid. Täiendavalt on tarvis koostada nimekiri riikliku sümboli staatuses veebisaitidest (nn monumentidest) ja riiklikest e-teenustest, mille majutamisel võiks kasutada avalikke pilvi.

Järgmisena on kavas **testida Eestile kriitiliste teenuste (nt ID-kaardiga autentimise teenus) ja elutähtsate teenuste opereerimist avalikus pilves**, et vältida olukorda, kus kriisi situatsioonis

[35] RIKS põhikiri, kättesaadav: http://riks.ee/529.html .
[36] Koostamisel olevast SF investeeringute kavast.
[37] DG CONNECT „Net-cloud futuure“, kättesaadav: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/NET-CLOUD_DIGITAL-AGENDA_clickable_0.pdf.
[38] „Implementation of the Virtual Data Embassy Solution. Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation.“ 2015, kättesaadav: https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf

proovitakse esimest korda, kas kriitiline teenus on pilvekõlbulik või mitte. Samuti viiakse läbi riigihange majutamaks osa riigi „monumente“ avalikke pilveteenuste pakkujate juures.

Eesti kohalikud omavalitsused vajavad selgeid juhiseid või läbimängitud kasutusstsenaariume oma asutuste IT-lahenduste tehnoloogiliseks ülesehitamiseks. Pideva eelarvekitsikuse ja suurmüüjate pakutavate litsentsitingimuste võimalustes tuleb vaatluse alla võtta olukorrad, kus pilveteenuste kasutamine oleks mõistlikum ja kulu-efektiivsem. Siinjuures pakub Eesti riik andmete krüpteerimiseks vajalikku infrastruktuuri ja kuigi enamus omavalitsuste hallatavast informatsioonist ei ole konfidentsiaalne, annab see siiski vajadusel võimaluse andmete turvaliseks krüpteerimiseks.

AKI on koostanud avaliku teabe seaduse üldjuhendi[39], mis kehtib ka pilveteenuste kohta. AKI täiendab juhendit andmete tervikluse säilitamiseks ja andmekaitse tagamiseks pilves vastavalt vajadusele. Täiendavalt tuleb RIAl koostöös MKMga töötada välja **spetsiifilised juhised ja meetmed, millistel tingimustel on serveriressursside või pilverakenduste erasektorilt ostmine mõistlik** ja milliste aspektidega tuleb seejuures arvestada.

3.4. Andmesaatkondade võrgustiku loomine

Andmesaatkondade võrgustiku loomine on pikaajaline projekt, mis tuleb ellu viia mitmes etapis. Esimene etapp hõlmab endas **andmesaatkondade võrgustiku asukohtade kindlaks määramist ning eeldab MKM ja VäM koostöökokkuleppe sõlmimist** konkreetsete saatkondade kasutamiseks andmesaatkondadena. Praeguseks ajaks on juba välja töötatud nii esialgsed tehnilised nõuded kui ka protseduurireeglid registrite ja rakenduste varundamiseks ja opereerimiseks.[40]

Kuna osa registreid eksisteerib Eestis üksnes digitaalsel kujul, on äärmiselt oluline tagada andmesaatkondadega Eesti digitaalne jätkusuutlikkus. MKMi juhitav küberjulgeoleku nõukogu, kuhu kuuluvad kõige olulisemad andmesaatkondade võrgustiku väljatöötamisega tegelevad partnerid, **peab määratlema kriitilise tähtsusega registrid ja teenused ning otsustama, kas vastav register või teenus vajab andmesaatkonnas või avalikus pilves majutamist ja varundamist**. Selleks tuleb nõukogul töötada välja registrite klassifitseerimise põhimõtted. Klassifikatsioonist tulenevalt teavad riigiasutused, kas neil tuleb viia oma registrid andmesaatkondadesse ja kui sageli nad peavad registreid seal uuendama. Nõukogul tuleb koostada nimekiri ka sellistest registritest ja teenustest, mis peavad olema kättesaadavad ja opereeritavad ligipääsu puudumisel Eestis asuvatele andmekeskustele.

Digitaalse järjepidevuse tagamiseks olulised infosüsteemid **tuleb määratleda riiklikke põhiregistritena** ning **töötada välja tegevuskavad** nende teenuste toimimiseks ohu- ja kriisiolukordades. Sealhulgas tuleb **leida lahendus kriitiliste andmete turvaliseks hoiustamiseks.**

Kui andmesaatkondade esimene etapp näeb ette üksnes Eesti riigi poolt kasutatava füüsilise saatkonna ruume, siis järgnevates etappides on plaanis kahepoolse lepingu alusel rajada andmesaatkonnad ka sõbraliku riigi andmekeskusse või luua Eesti virtuaalsaatkond sõbraliku riigi pilve**. Andmesaatkondade**

[39] AKI „Avaliku teabe seaduse üldjuhend“, kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Avalku%20teabe%20seaduse%20%C3%BCldjuhend%20%2822.10.2014%29_2.pdf

[40] RIA ja VäM 26.02.2015 töökohtumise protokoll.

võrgustiku loomise ulatus lepitakse kokku küberjulgeoleku nõukogus ning see sõltub esimese etapi tulemustest ja kulubaasist.

4. Riigipilve rakendusplaani riskid

4.1. Riskikeskkond

Riigipilve rakendusplaani elluviimisel tuleb erilist tähelepanu pöörata järgnevate operatsiooniriskide juhtimisele:

- **Õiguslik- ehk regulatiivrisk -** võimalus, et pilveteenuse kasutamine läheb vastuollu kehtivate seaduste ja regulatsioonidega. Antud risk on asjakohane eelkõige seetõttu, et tehnoloogia kiire arengu tõttu ei võta valdav osa regulatsioonidest arvesse pilvandmetöötluse võimalust ning sellise tehnoloogia kasutamine võib minna vastuollu regulatsiooni nõuetega, isegi juhul kui selle tehnoloogia kasutamine ei too tegelikult kaasa kellegi huvide kahjustamist.
- **Reputatsioonirisk –** võimalus, et pilveteenuse rakendamisel tekkinud häired kahjustavad teenuse mainet niivõrd, et selle kasutajad loobuvad sellest üldse.
- **Kontsentratsioonirisk -** võimalus, et andmete ja teenuste koondumine ühte füüsilisse punkti või ühe teenusepakkuja kätte võimendab ühes punktis toimuva intsidendi kahjulikku mõju suuremale hulgale andmetele.
- **Teenuste sisseostu- ja tarneahela risk** – võimalus, et pikenenud ahel teenuse pakkuja ja tarbija vahel toob vastutuse hajumise ning suure protsessiosaliste hulga tõttu kaasa kõrgema intsidendiriski.

4.2. Riskide juhtimine

Riigipilve rakendusplaani elluviimisel tuleb lähtuda konservatiivsetest riskijuhtimise printsiipidest, lähtudes üldtunnustatud riskijuhtimise tavadest (nt lähtuvalt EVS-ISO 31000:2010 ja EVS-EN 31010:2010 põhimõtetest). Oluline on tagada järgnevate põhimõtete täitmine:

- iga riikliku teenuse omanik, kes asub pilvetehnoloogiat kasutama peab ise läbi viima põhjaliku ja igakülgse riskianalüüsi;
- teenuse sisseotsmisel tuleb teostada teenusepakkuja reputatsiooni, tehnilise võimekuse ja jätkusuutlikkuse hindamine (*due diligence*);
- teenuse sisseostmisel tuleb teenustaseme lepingu väljatöötamisel hinnata teenusepakkuja tegelikku valmidust käideldavuse, konfidentsiaalsuse ja terviklikkuse tagamiseks;
- operatsiooniriskide hindamine peab toimuma konservatiivselt ja kooskõlas üldtunnustatud riskijuhtimise tavadega;
- õiguslike- ja regulatiivriskide maandamine saab toimuda ainult täieliku vastavuse põhimõttel, s.t riigiasutus ja avaliku teenuse osutaja ei saa võtta riski seadust või regulatsiooni eirata. Juhul kui regulatsioon on ilmses vastuolus avaliku huviga ja aegunud, tuleb põhjendatud avaliku huvi korral algatada regulatsiooni muutmine;

- teenuse intsidendihalduse-, taaste- ja varundusplaanid peavad arvestama avalike teenuste eripärasid ja suurt avalikku huvi intsidentide vastu.

5. Kokkuvõte

Eesti riik on rajanud kindla aluse infoühiskonna toimimiseks ning arenguks ja siinne elanikkond on info- ja kommunikatsioonitehnoloogia funktsioneerimisest igapäevaselt sõltuv.

Samas on teenuseid ja lahendusi arendades vältimatu arvestada kaasaegsed ja tulevikku vaatavaid võimalusi, mis omakorda tingib vajaduse paindliku riigipilve lahenduse järele. Riigi serveriruumide konsolideerimine standarditele vastavatesse andmekeskustesse, erasektori ressursside paindlik kaasamine nii Eestis kui ka väljaspool riigi piire ja andmesaatkondade võrgustiku rajamine loovad Eesti riigipilve rakendumiseks tugeva aluse, tagades senisest kvaliteetsemad teenused, digitaalse järjepidevuse ja suurema turvalisuse. Riigipilve kontseptsiooni rakendamine toob kaasa ka olemasolevate infosüsteemide kaasajastamise ja uuendamise, et need oleksid suutelised pilvetehnoloogia pakutavaid võimalusi kasutama.