Riigi IT Keskus

Microsoft riskianalüüs

Kirjeldus

Microsoft Corporation (edaspidi Microsoft) on Ameerika Ühendriikide (USA) tehnoloogiaarendusettevõte, mille peakorter asub Washingtoni osariigis Redmondi linnas. Ettevõte arendab, toodab, litsentseerib ja müüb mitmesuguseid IT-seadmeid ja tarkvara. Samuti pakutakse klientidele tehnilist tuge ning muid teenuseid. Microsoft on asutatud 1975. aastal ning pilvetehnoloogiate valdkonnas üks juhtivaid ettevõtteid, mille perspektiiv teenuseid pikaajaliselt pakkuda on kõrge.

Microsoft tegutseb Eestis, Tallinnas (Microsoft Estonia OÜ) alates 2003. aastast, kuid tooteid müüakse läbi kohalike edasimüüjate.

Käesolev riskianalüüs keskendub Microsoft pilvtöötlusteenuse (edaspidi pilv ja sellega seotud teenus ehk pilveteenus) riskide kirjeldamisele ning ei kohaldu toodetele, mida on võimalik kasutada asutuse sisestel ressurssidel.

Microsoft pilve võimalused

Microsoft pilveteenused on ülemaailmselt kasutusel, laia kasutajabaasiga ning toodete (M365 tooted) kasutusele võtmine ei eelda kasutajatelt reeglina täiendavat väljaõpet. Microsoft pilveteenused on kasutajasõbralikud ja lihtsalt kasutatavad.

Microsoft pilveteenused võimaldavad asutustel vähendada vajadust omada ja hooldada kohapealset IT-infrastruktuuri, mis võib kaasa tuua märkimisväärseid kulude kokkuhoiuvõimalusi. Asutused saavad kasutada pilveteenuseid vastavalt vajadusele, kasvades või vähenedes vastavalt nõudlusele ja maksta ainult selle eest, mida nad tegelikult kasutavad.

Microsoft pilveteenused võimaldavad hallata suures mahus seadmeid (serverid, tööjaamad, nutiseadmed), kasutajale suunatud teenuseid (*OneDrive, Sharepoint, Teams jms*), kasutajate identiteete ja ligipääse (*Azure AD, PIM*) ja erinevaid ressursse (nt litsentsid, *Single Sign-On* ja ühendused teiste teenustega, turbeteenused, automatiseerimisvahendid jms).

Microsoft pilveteenused võimaldavad juurde pääseda mis tahes interneti ühendust omavast seadmest või piirata ligipääsu kindlatelt aadressidelt. Microsoft pilveteenuseid värskendatakse automaatselt ja regulaarselt uute funktsioonide ja veaparandustega, mis välistab vajaduse uuendusi käsitsi rakendada ja võimaluse, et kasutusel on aegunud tarkvara versioon. Igal Microsoft kliendil (antud juhul käsitletakse kliendina Eesti riiki, kuid võimalik on luua kliente ka madalamal tasemel, nt asutus) on enda keskkond, mis ei puutu kokku teiste Microsoft klientide andmetega.

Microsoft investeerib pidevalt pilveteenuste arengusse ja tootearendusse, pakkudes juurdepääsu uutele tehnoloogiatele ja funktsioonidele. See võimaldab kasutada täiustatud tarkvara/riistvara, tehisintellekti, analüütikat ja andmeid, et parandada teenuste pakkumist, tõhustada töövooge ja teha paremaid otsuseid.

Microsoft pilveteenuseid saab integreerida mitmete teiste ettevõtete tööriistade ja teenustega, sh populaarsete projektihaldus- ja tootlikkuse tööriistadega (nt *Atlassian, AWS* jms).

Microsoft pilveteenused võimaldavad asutustel kasutada võimsaid arvutusvõimsusi, andmetöötlusteenuseid, koostöövahendeid ja muid tööriistu, mis parandavad efektiivsust ja suurendavad tootlikkust. Asutused saavad kiiremini käivitada uusi projekte, vähendada IT-infrastruktuuri haldamisega seotud koormust ja võimaldada töötajatel paindlikult ja turvaliselt töötada.

Skoor: võimaldab optimeerida baasteenuste kulusid ning maandab tarkvara uuendamisest tulenevaid turvariske– 4 (kõrge)

Microsoft pilve puudused

Microsoft pilveteenuseid majutatakse väljaspool Eesti territooriumi ning vajavad üldiselt toimimiseks püsivat interneti ühendust. Ühenduseta Microsoft pilve (nt saartalitluse olukorras või olukorras, kus Microsoft teenus ei toimi) on teenuste toimimine võimalik ainult osas, kus infot ajutiselt salvestatakse kohalikku seadmesse (nt Windows turvaseaded, Windows autentimispiletid, kohalikule kettale salvestatud failid (kasutades *OneDrive'i*) jms), kuid pikaajalise katkestuse korral on vajalikud alternatiivsed rakendused (nt *on-prem Active Directory* toimimine, võimalus e-posti ümber suunata *on-prem* serverisse, alternatiivse ja/või on-prem suhtlusrakenduse kasutamine jms). Eesti riigiasutuste jaoks on oluline teabevahetuse korraldamine ka olukordades, kus välisühendused halvatakse kas pahatahtliku ründe tõttu või on sunnitud riik ennetava meetmena ise ühendused katkestama[1].

Microsoft pilve kasutamisel saab ettevõttest isikuandmete (all)volitatud või teine volitatud töötleja, kelle andmekeskused paiknevad osaliselt USA-s ning Microsoftiga lepingut sõlmides ei ole võimalik kliendil oluliselt mõjutada lepingutingimusi. USA-s tegutsevatele isikutele ja asutustele ja/või USA-s asuvatesse andmekeskustesse isikuandmete edastamine ei ole üldjuhul lubatud, sest Euroopa Liidu ja USA vahel ei ole alates 2020. aasta juulikuust[2], mil Euroopa Kohus tunnistas kehtetuks *Privacy Shield'i* nimelise andmekaitseraamistiku, toimivat andmekaitsealast koostööd ning andmete edastust. Sellega seoses ei ole andmesubjektidele USA-s toimuva andmetöötluse osas tagatud samaväärsed õigused (ei pruugi olla tagatud turvameetmed, võidakse teostada andmekorjet või edastada andmeid kolmandatele isikutele, nt järelevalveasutused, vt ka *CLOUD Act*[3]), nagu kehtivad Euroopa Liidus toimuva andmetöötluse suhtes. Töö uue vastava andmekaitseraamistiku loomise nimel käib siiski aktiivselt ja selle heakskiitmist võib prognoosida 2023. aasta jooksul[4]. Microsoft pilv võimaldab riski maandamiseks andmeresidentsuse[5] asukohaks valida Euroopas asuvad serverid.

Microsoft teenuseid kasutab valdav osa maailma riikide avaliku sektori asutusi ning suurkorporatsioone, mis muudab Microsoft pilve oluliseks sihtmärgiks pahatahtlikele osapooltele (nt riiklikult sponsoreeritud rühmitused), kelle

[1] https://www.aki.ee/sites/default/files/ringkirjad/andmetootlusest_avalikes_pilveteenustes_0.pdf

[2] EKo 16.07.2020, C-311/18 – Data Protection Commissioner vs Facebook Ireland Ltd, Maximillian Schrems

[3] https://en.wikipedia.org/wiki/CLOUD_Act

[4] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_et

[5] https://azure.microsoft.com/en-us/explore/global-infrastructure/data-residency/#overview

eesmärgiks on läbi Microsoft taristu saada ligipääs Microsoft klientide andmetele. Ohu maandamiseks on Microsoftil 24/7 toimiv *Cyber Defense Operations Center* (*CDOC*)[6] ning lisaks Microsofti integreeritud turvatoodetele on loodud võimalused Microsoft pilvega integreerida kolmanda osapoole turvatooteid.

Microsoft pakub pilves märkimisväärset hulka rakendusi (*Azure AD*, e-post, kalender, suhtlusrakendus, koostöörakendus jms), mille haldamiseks ja administreerimiseks on igale rakendusele võimalik määrata rohkeid (turva)seadistusi. Enam kasutatavate rakenduste puhul (nt *Intune, Teams* jms) on võimalik seadistada rohkem kui 1000 erinevat poliisikat, millega kogupoliisikate arv ületab tõenäoliselt 10 000 piiri. Poliisikate ning nende seoste haldamine, nende mõistmine, testimine, turvaline rakendamine, dokumenteerimine ja jälgimine on märkimisväärselt keeruline ülesanne, mille kompetentseks teostamiseks on vajalik pidev väljaõpe, partnerluslepe Microsoftiga ning Microsoft pilvele spetsialiseerunud meeskond.

Microsoft pilv kasutab vaikimisi andmete krüpteerimiseks Microsoft poolt loodud ja hallatud RSA turvavõtmeid, mille pikkus saab olla 1024 või 2048 bitti. Vastavalt RIA krüptouuringus[7] viidatule on 2048 bitiste võtmete kasutushorisondiks aasta 2030, peale mida ei saa garanteerida andmete salajasust. Seejuures on oluline, et krüptograafiline võti, mida on vaja andmete dekrüpteerimiseks, asuks vastutava töötleja ainuvalduses. Kui see selliselt korraldatud ei ole, ei saa järeldada, et krüptograafia rakendamine koos andmekaitse standardklauslitega tagaks nõutud tasemel kolmanda riigi, sh USA õigusruumist tulenevad riskid. Käesolevalt ei ole Microsoft pilve võtmed vastutava töötleja ainuvalduses. Riski on võimalik aktsepteerida, kuna Microsoft pilve kasutamist on võimalik vajadusel vältida (kasutades tundlike andmete jaoks *on-prem* lahendusi) või kasutada eraldiseisvat krüpteeringut (nt ID-kaardi krüpto), mis muudab andmed Microsoftile loetamatuks.

Skoor: tööprotsesside seisak, süsteemide funktsionaalsus andmete tervikluse ja salajasuse tagamine – 4 (kõrge)

Microsoft pilve kasutamise mõju kasutajale

Kasutajad eelistavad Microsoft pilverakenduste kasutusele võtmist, kuna pilverakendused pakuvad rohkem funktsionaalsust ning on kaasaegsemad (nt *Skype for Business vs Teams*). Mõju on pikas perspektiivis positiivne, Microsoft pilverakenduste kasutusele võtmine tõstab tõenäoliselt töötajate produktiivsust ning võimaldab tööülesandeid täita paindlikumalt (nt kasutades lisaks arvutile nutiseadmeid).

Microsoft pilve kasutamisel võib olla negatiivne mõju, eelkõige Microsoft pilve kättesaadavuse katkemisel avalikele teenustele ja võimaliku väärkasutamise mõju. Kuna selle mõju ulatus on suur, võib tekkida oht riigi julgeolekule, kui puuduvad piisavad alternatiivid Microsoft pilveteenusele. Mõju täpsemaks hindamiseks on võimalik kasutada Microsoft teenuste käideldavusinfot[8].

Skoor: positiivne mõju protsessidele – 4 (kõrge)

[6] microsoft.com/en-us/msrc/cdoc

[7] https://www.ria.ee/media/3041/download

[8] https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1&year=2023

Rahaline mõju

Microsoft pilve kasutamine on teatud piirini kulutõhus, kuna Microsoft litsentsipakett tuleb kasutajatele soetada Office rakenduste kasutamiseks (mida ei ole otstarbekas asendada mõne muu (vabavaralise) rakendusega, näiteks *LibreOffice*) ning valdavalt kasutatavate litsentsipakettidega (A3/E3) kaasnevad täiendavad funktsioonid (nt pilves majutatud Microsoft Teams) ja ressursid (nt igal kasutajal on 100GB pilve-postkast). Microsoft teenuste litsentsikulud suurenevad pidevalt, keskmiselt on iga kolme aasta tagant tehtava riigihanke hind ca 20% kõrgem eelmisest perioodist.

Kulud kasvavad oluliselt kui:

- on vajadus rakendada täiendavaid turbemeetmeid (nt Defender lisafunktsionaalsused, Sentinel, Information Boundaries jms);
- kui kasutaja või asutuse vaates ületatakse ette antud mahtusid (nt postkastis, Sharepointis jms teenustes);
- juhul kui asutus kasutab palju osalise töökoormusega töötajaid (Microsoft litsentseerib igat individuaalset isikut);
- kui rakendamisel on vaja kaasata Microsoft täiendavat tuge (nt Unified Support);
- kui asutusel on vajalik valida, millises riigis tema andmeid töödeldakse;
- kui riigi siseselt või asutusel on vajalik eraldada enda ressursse erinevate Microsoft pilveinstantside vahel, loob eraldamine täiendavat keerukust haldamisele ja administreerimisele.

Skoor: täiendav kulu eelarves – 4 (kõrge)

EL/NATO liikmesriigis hoitavad andmed

Microsoft peakontor asub USAs, aga klientide andmete asukoht on kliendi enda valida, vaikimisi asuvad Eesti kasutajate andmed Euroopa Liidus (täpsustamata asukoht). Andmeid on võimalik hoida erinevates regioonides, sh valiku tegemiseks Euroopa Liidu siseselt on vajalik täiendav litsentseerimine[9]. Siiski ei ole võimalik olla 100% veendunud, et kõik kliendi andmed (sh metaandmed) asuvad igal ajahetkel Euroopas. *GDPR-i* kohaselt võib andmeid edastada väljapoole Euroopa Liitu kui on rakendatud asjakohased kaitsemeetmed (artikkel 46[10]).

Skoor: võimalik valida, kus andmeid hoida – 4 (kõrge)

Teenusest lahkumise ja andmete ekspordi võimalus

Microsoft pilve teenusest on võimalik lahkuda ja andmed eksportida, samas sõltub selle teostatavus konkreetsest rakendusest ning selle võimalikest alternatiividest. Näiteks on võimalik mõistlike pingutustega lahkuda Microsoft e-posti teenusest kui on olemas teenus, kuhu suunata uute kirjade vastuvõtmine ning migreerida andmed (näiteks *Google Workspace'i*[11]). Samas on tõenäoliselt ebamõistlik migreerida andmeid Microsoft Teams'ist mõnda muusse rakendusse, mistõttu on otstarbekam andmed arhiveerida ning alustada uue teenusega ilma varasemate andmeteta.

Andmekao vältimiseks peaks andmete omanik hindama igas Microsoft pilveteenuses olevat andmete koosseisu ning nende ajaloolist väärtust, et hinnata,

[9] Advanced data residency in Microsoft 365 - Microsoft 365 Enterprise | Microsoft Learn

[10] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&qid=1689851996164

[11] Migrate from Exchange or Exchange Online to Google Workspace - Google Workspace Admin Help

kas andmete eksportimine on vajalik ja otstarbekas.

Microsoft teenuse lõpetamisel on aega andmete migreerimiseks 90 päeva (sh 30 päeva on teenus tavapäraselt kasutatav), kliendi andmed ja nende koopiad kustutatakse Microsoft teenusest 90-180 päeva pärast[12]. Teadaolevalt puuduvad Microsoft pilves tõendusmeetmed kõigi kliendi andmete kustutamise kohta ning tuleb eeldada, et peale kustutamist jäävad andmed Microsoftile kättesaadavaks.

Skoor: võimalik teenusest lahkuda ja eksportida andmeid – 4 (kõrge)

Vastavus sertifikaatidele (ISO, E-ITS jms)

Microsoft on sertifitseerinud protsessid ning erinevad teenused paljude rahvusvaheliselt tunnustatud metoodikate vastu. Muuhulgas on Microsoft sertifitseerinud kõik olulisemad teenused, mida Eesti avalikus sektoris kasutatakse:

- Azure (nt ISO 27001:2022 ja paljud muud)[13];
- Office 365 (nt ISO 27001:2013 ja paljud muud)[14].

Skoor: olemasolevad sertifikaadid on vastavuses KüTS nõuetega – 5 (kõrge)

Andmekaitse meetmete rakendamine

Microsoft pilve kantud andmed on krüpteeritud kuni 2048 bitise võtmega (vt sektsioon „Microsoft pilve puudused"). Andmeid anonümiseeritakse teatud ulatuseni Microsoft enda poolt (nt süsteemilogid)[15] ning osades teenustes on võimalik kliendil valida andmete anonümiseerimine (nt *Defender for Cloud* teenuses[16]).

Teadaolevalt krüpteeritakse vaikimisi kõiki andmeid Microsoft pilveteenuste ja kasutaja vahel nende edastamisel (standardsed *SSL* lahendused, nt veebilehitseja ja veebiteenuse vahel).

Enamik Microsoft pilveteenustest on mitme rentnikuga teenused, mis tähendab, et andmeid, juurutuskomplekte ja virtuaalarvuteid võidakse talleta samas füüsilises riistvaras, kus talletatakse ka teiste klientide omi. Microsoft rakendab loogilist isoleerimist, et eraldada eri klientide talletus- ja töötlusandmed. Selleks kasutatakse eritehnoloogiaid, mis aitavad tagada, et kliendiandmeid ei kombineerita teiste klientide andmetega. Täiendava turvalisuse saavutamiseks on võimalik rakendada BYOK (*bring your own key*)[17].

Skoor: andmekaitsetingimused on täidetud – 4 (kõrge)

[12] What happens to my data and access when my subscription ends? | Microsoft Learn
[13] Azure compliance documentation | Microsoft Learn
[14] ISO/IEC 27001:2013 Information Security Management Standards - Microsoft Compliance | Microsoft Learn
[15] Continuing Data Transfers that apply to all EU Data Boundary services - Microsoft Privacy | Microsoft Learn
[16] Cloud Discovery data anonymization - Microsoft Defender for Cloud Apps | Microsoft Learn
[17] Bring Your Own Key (BYOK) details - Azure Information Protection | Microsoft Learn

Andmekaitsetingimused

Teadaolevalt toimub Microsoft pilves kõigi kliendi andmete töötlemine automaatselt ning klientide andmeid töödeldakse automatiseerimata vahenditega ainult erandjuhtudel (nt kliendi pöördumise lahendamiseks).

Microsoft pilveteenuste puhul töödeldakse kliendi isikuandmeid. Kui Microsoft tellib alltöövõtjalt teenuseid, mille käigus need võivad saada ligipääsu nimetatud andmetele, loetakse alltöövõtjad volitatud andmetöötlejaks. Microsoft avalikustab alltöövõtjad.

Microsoft pilv on vastavuses *GDPR-i* nõuetega[18]. Microsoft teavitab klienti pilveteenuses toimuvatest sündmustest ning Microsoft iseteeninduses on kliendil võimalik määrata asutuse andmekaitsekontakti, kelle poole Microsoft saab täiendavalt pöörduda[19].

Microsoft on valmis aitama klienti, kui kliendil on vaja vastata andmesubjekti pöördumistele, st andmete kustutamise, parandamise, töötlemise piiramise korral.

Avaliku teabe seaduse (edaspidi AvTS) § 34 lõike 2 kohaselt võib asutuse juht kehtestada konkreetsele teabele juurdepääsupiirangu, tunnistades vastava teabe AK teabeks. AK teabele on AvTS § 38 lõike 3 kohaselt juurdepääsuõigus vaid riigi ja kohaliku omavalitsuse ametnikul või töötajal oma ametiülesannete täitmiseks. Sama sätte kohaselt ei tohi AK teavet ilma juurdepääsupiirangu kehtestanud asutuse loata edastada kolmandatele isikutele.

Isikuandmete puhul leidub kehtivas õiguses *GDPR* artiklist 28 tulenev õiguslik alus volitatud töötlejate kaasamiseks andmetöötlusprotsessi, kuid seejuures tuleb lähtuda volitatud töötlejale kehtestatud nõuetest (MKM õigusanalüüs, p 53).

Kui volitatud töötleja poolt kaasatud teine volitatud töötleja ei täida oma andmekaitsekohustusi, jääb algne volitatud töötleja *GDPR* artikli 28 lõike 4 kohaselt vastutava töötleja ees teise volitatud töötleja kohustuste täitmise eest täielikult vastutavaks.

Skoor: andmekaitse tagamine on kooskõlas määrusega – 4 (kõrge)

Turvameetmete rakendamine

Microsoft rakendab oma toodete turvalisuse tagamiseks erinevaid meetmeid:

- Microsoft opereerib enda toodete turvalisuse tagamiseks turbemeeskonda (*CDOC*) ning on rakendanud meetmed turbeintsidentide lahendamiseks[20];
- Microsoft on rakendanud *Bug Bounty* programmi[21] vigadest raporteerimiseks;
- Microsoft on loonud avaliku sektori asutustele suunatud *Government Security Program (GSP)*[22] turbealase info jagamiseks;
- Microsoft protsessid ning tooted on sertifitseeritud hulga rahvusvaheliselt tunnustatud metoodikate vastu ning kodulehel on avaldatud ka olulisemad põhimõtted turbe tagamisel (nt füüsiline ligipääs andmekeskustele[23]);
- Microsoft teenuste kasutamisel on võimalik kliendil kasutusele võtta

[18] General Data Protection Regulation - Microsoft GDPR | Microsoft Learn
[19] Breach Notification - Microsoft GDPR | Microsoft Learn
[20] Security incident management overview - Microsoft Service Assurance | Microsoft Learn
[21] Microsoft Bounty Programs | MSRC
[22] Government Security Program (microsoft.com)
[23] https://learn.microsoft.com/en-us/compliance/assurance/assurance-datacenter-physical-access-security?source=recommendations

enamlevinud turvalise töötlemise vahendid (nt mitmetasemeline	autentimine, tingimuslikud ligipääsud jms).

Skoor: rakendatud turvameetmed muudavad teenuse kasutamise ohutumaks – 5 (kõrge)

Riskid

Pilvega seotud riskid	Pilveteenuse pakkuja IT süsteemi avarii tõttu ei suudeta pakkuda teenust vastavalt kokkulepitud käideldavusnõuetele ja andmeid ei ole võimalik taastada kokkulepitud ulatuses. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu püsivalt Microsoft pilveteenuse toimimisest. Olemas on plaanid töötamaks ilma pilveteenusteta.**
	Pakutav teenus ei ole ajakohane. SAAS pilveteenuse puhul vastutab uuenduste eest pilveteenuse pakkuja, muudel juhtudel võib vastutus langeda ka teenuse tellijale. Ise teenust majutades on oht, et rakendus ei saa piisavalt kiirelt uuendusi. **Microsoft *on-prem* lahenduse kasutamine on aeglasem ja väiksemate funktsionaalsustega, kui pilveteenuses. Microsoft pilveteenust hoiab teenusepakkuja ajakohasena.**
	Teenuse osutamise ebapiisav järelevalve. Pilveteenuse pakkuja poolt osutatav teenus ei vasta käideldavuse ja tervikluse nõuetele. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu ainult Microsoft pilveteenuse toimimisest.**
	Teenusepakkuja turvameetmete ebapiisav järelevalve. Järelevalve puudumisel muutuvad avalikuks konfidentsiaalsed ja delikaatsed andmed. **Microsoft pilveteenused on läbinud infoturbe auditid ja vastavus tuntud standarditele.**
	Teenuse õiguste jagamisel tehakse vigu. Administreerimisel tehakse inimlikke vigu. Rollide jagamise protsess on puudulik (pääsuõiguste protsess). **Asutuse IAM rakendamine, kasutajaõiguste automaatne haldamine.**
	Teenuse seadistamisel tehakse vigu. Seadistaja vea või teadmatuse tõttu seadistatakse teenus ebaturvaliselt. **E-ITS rakendamine ning vajadusel turbetestimine.**
	Teenust ei kasutata tõhusalt. Ei võeta kasutusele kõiki paketiga kaasa tulenevaid võimalusi (turvanõudeid, teenuseid jne). Pilveteenuse seadistamisel tuleb määrata turvanõuded, mis valitud paketi/teenusega kaasa tulevad (nt kaheastmeline autentimine (***2FA***), nutiseadmesse lisaparooli lisamine, ***FIDO2*** võtmed jne). **E-ITS rakendamine ning sellest tulenev kaasaegsete autentimisvahendite ja turvanõuete kasutamine. Administraatorite koolitamine Microsoft pilveteenuste turvaliseks seadistamiseks ja kasutamiseks.**
	Teenuse kasutamine on ebamugav ja keerukas. Teenuse juurutamisel kasutajad jäävad koolitamata. Hakatakse otsima erinevaid lihtsamaid alternatiive dokumentide arhiveerimiseks või taastamiseks.

Pilvega seotud riskid	**Teadlikkuse tõstmine Microsoft pilveteenuste kasutamisel, üksikute teenuste ning laiema kasutuselevõtu korral teenuse peakasutaja määramine.**
	Välise teenusepakkuja poolne andmete lekitamine kolmandale osapoolele. Teenusepakkuja lubab ligipääsu salajastele andmetele. **Asutuse poolne *BYOK* rakendamine.**
	Töötajate lahkumine või liikumine organisatsioonis. Süsteemi tundev inimene lahkub või on eemal. Ei ole samade oskustega asendajat. **Teadlikkuse tõstmine ja koolitused teenuse kasutamiseks.**
	Pilveteenuse väärkasutus. Tundlike dokumentide saatmisel/jagamisel sisestatakse vale inimese kontaktid, jagatakse ***read-only*** dokumente muutmisõigustega, tehakse näiteks dokument kogemata avalikuks või unustatakse dokumendid krüpteerida. Inimesed ei ole piisavalt koolitatud või teadlikud, et teenust turvaliselt kasutada. ***BYOK* rakendamine, kasutajate pidev koolitamine ja teadlikkuse testimine.**
	Internetiühenduse katkemine lõppkasutajal. Internetiühenduse katkemine sideteenusepakkuja rikke/vea tõttu. Ei ole võimalik ligi pääseda pilveteenuses asuvatele andmetele. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu püsivalt Microsoft pilveteenuse toimimisest**.
	Teenust pakkuv server ei vasta. Ei ole võimalik pilveteenusele ligi pääseda teenusepakkujapoolse võrgukatkestuse tõttu. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu püsivalt Microsoft pilveteenuse toimimisest**.
	Ei varundata teenuses hoitavaid andmeid. Varukoopiate puudumisel ei ole võimalik andmeid taastada. **Teenuspakkuja poolt tagatud andmete ekspordi ja varundamise võimalus.**
	Ressursside jagatud kasutuse riskid. Pilveteenuse kliendid jagavad samu ressursse- servereid, võrku, salvestusruumi. Erinevate klientide eraldamine on pilveteenuse osutaja ülesanne ning sõltub tema süsteemide ja protsesside turvalisusest. On võimalik, et kliendid saavad teatud tingimustel infot teiste klientide teenuste andmevahetuse või salvestatud andmete kohta. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Teenuste koormatuse tõus. Pilveteenuse pakkuja ei suuda koormuse tõttu kokkulepitud käideldavuse nõudeid tagada, mille tõttu ei ole andmed kättesaadavad. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu püsivalt Microsoft pilveteenuse toimimisest**.
	Andmete või tarkvara manipuleerimine rünnaku tagajärjel, nt turvanõrkuste olemasolul, teenuse pahatahtlik väärkasutus, ***DDoS.*** Ründed pilveteenusepakkuja vastu. Avalik haldusliides (andmevahetus), paroolide lekkimisel rünnatav. Pilveteenuse pakkuja ei suuda kokkulepitud käideldavusnõudeid tagada. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu püsivalt Microsoft pilveteenuse toimimisest**.

Isikuandmetega seotud riskid	Väliste teenuste volitamata kasutamine. Pilveteenuse pakkuja kasutab väliseid teenusepakkujaid, kellele esitatud infoturbenõuded ei vasta teenuse terviklikkuse ja käideldavuse nõuetele. Lubatakse ligipääs salajastele andmetele või autentimise infole. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Administraatori õiguste väärkasutus. Pilveteenuse pakkuja IT administraatorite õiguste volitamata kasutamine võib kaasa tuua andmekao või andmete muutmise/hävitamise. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Andmekaitseseaduste eiramine. Euroopa Liidu isikuandmete kaitse üldmäärusest ning kohalduvatel juhtudel isikuandmete kaitse seadusest või muudest regulatsioonidest tulenevad nõuded isikuandmete töötlemisele. Oht tekib, kui organisatsioon eirab isikuandmete töötlemisel rakenduvaid andmekaitsenõudeid, mille eesmärk on andmesubjekti õiguseid kaitsta, näiteks töödeldes andmeid eesmärgita, läbipaistmatult, turvameetmeid rakendamata või ilma andmesubjekti sekkumisvõimaluseta. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Isikuandmete ebapiisav turve veebirakendustes. Isikuandmete lekkimine. **Kasutatakse krüpteerimist, pseudonüümiseerimist, anonüümiseerimist. Rakendatakse uuemaid ja kaasaegsemaid infotehnoloogilisi turvameetmeid. Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Puudulikud andmetöötlusprotseduurid. Andmete väärkasutamise oht kasvab, kui organisatsioonis puuduvad protseduurid IT-süsteemidele ja andmetele õiguspärase juurdepääsu tagamiseks või kui andmete kasutamine ei ole logide ega dokumentatsiooni abil tõendatav. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Puudulik privaatsus. Isikuandmete töötlemine võib riivata andmesubjekti õigust perekonna- ja eraelu puutumatusele. Eriti võib selline riive tekkida, kui töödeldakse eriliiki isikuandmeid ehk isikuandmeid mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või maailmavaatelisi tõekspidamisi ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning biomeetria kohta. Puudulik privaatsus tähendab isikuandmete töötlemist viisidel, mille rakendamine, rakendamisega seotud tegevused või tegevusetus, või rakendamisest tulenevad tagajärjed, sealhulgas kõrgendatud oht isikuandmetega seotud rikkumise toimepanemisele, põhjustab õigusvastase riive andmesubjekti õigusele perekonna- ja eraelu puutumatuse vastu. Näiteks võib tekkida õigusvastane privaatsuse riive olukorras, kus õigusliku aluseta tutvutakse inimese andmetega mõnes andmekogus. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**

Isikuandmetega seotud riskid	Puuduv või puudulik andmekaitsekontroll. Avastamata rikkumised ning lubamatu andmete töötlemine. Mainekahju organisatsioonile. Kahjunõuded ja trahvid. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Isikuandmete hankimine ilma seadusliku aluseta või isiku nõusolekuta. Õigusaktide rikkumine. Organisatsioonile mainekahju ja rahaline kahju. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Isikuandmete kasutamine muuks kui hankimiseks lubatud otstarbeks. AK andmete levitamine/lekitamine. Kahjunõuded, rahalised trahvid ning mainekahju. Nt logiandmeid ei tohi koguda selleks, et tuvasta kasutajate harjumusi. Andmeid kogutakse ja kasutatakse minimaalselt (nii vähe kui võimalik) ja säilitatakse üksnes seniks, kuni neid vajatakse. Piiratakse andmetele juurdepääsu (nii organisatsiooni siseselt kui väliselt). **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Isikuandmete lubamatu edastamine. AK andmete levitamine/lekitamine. Kahjunõuded, rahalised trahvid ning mainekahju. **Rakendatakse uuemaid ja kaasaegsemaid infotehnoloogilisi turvameetmeid. Piiratakse andmetele juurdepääsu (nii organisatsiooni siseselt kui väliselt), nt kasutades pseudonümiseerimist ja krüpteerimist. Töötajate koolitamine**.
	Isikuandmete liigne kogumine. Õigusaktide rikkumine. Organisatsioonile mainekahju ja rahaline kahju. Andmeid kogutakse ja kasutatakse minimaalselt (nii vähe kui võimalik) ja säilitatakse üksnes seniks, kuni neid vajatakse. Piiratakse andmetele juurdepääsu (nii organisatsiooni siseselt kui väliselt). **Tagatakse korrapärane isikuandmete kustutamine pärast säilitusaja lõppemist.**
	Andmetöötlusprotsessi ebapiisav või puuduv kaitse isikuandmete töötlemisel välisriikides. Trahvid ja kahjunõuded ning mainekahju organisatsioonile. Andmete töötlemine ilma aluseta või valedel põhjustel. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Puudulik läbipaistvus andmekaitse kontrolliinstantside ja asjakohaste isikute jaoks. Päringute suurenemine, mis takistab tööprotsessi. Trahvid ja rahaline kahju organisatsioonile. Rakendatakse uuemaid ja kaasaegsemaid infotehnoloogilisi turvameetmeid. Luuakse lahendusi, kus isikud saavad kergemini oma andmete ligi (nt e-teenindus). **Asutus loob läbipaistvad kasutustingimused, mis annavad ka isikule endale võimaluse enda turvalisuse eest paremini seista.**
Tarkvaraga seotud riskid	Ohtlikest riikidest hangitud tark- ja riistvara. Teenusepakkuja kasutab nt riist- ja tarkavara ohtlikest riikidest. Mainekahju organisatsioonile. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**

Tarkvaraga seotud riskid	Andmekaotuse tõttu tekkiv käideldavuse kadu. Andmete kaotuse tõttu võivad mingid protsessid välja langeda ning organisatsioon võib lähtuda väärotsustest. Tekkida võib ka maine- ja rahalinekahju. **Asutuse töö on korraldatud selliselt, et toimimine ei sõltu püsivalt Microsoft pilveteenuse toimimisest**.
	Andmete ettevaatamatu või lubamatu kustutus. Vale hoolduse, väärtalituse, toitekatkestuse, saaste või kahjurvara tõttu võivad andmed kustuda. **Asutus ei säilita Microsoft pilveteenuses andmetest ainukoopiaid, millest sõltub teenuste pakkumine. Andmetest tehakse varukoopiaid.**
	Tarkvara päritolu mitte kontrollimine. IT-süsteemid võivad nakatuda kahjurvaraga. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
	Ebausaldatavast allikast pärit teave või tooted põhjustavad valeandmetel või vigastel arvutustel põhinevat väärotsust või konfidentsiaalsete andmete lekete. **Teenusepakkuja poolt läbitud turbeauditid ja vastavus tuntud standarditele.**
Andmekaotusega seotud riskid	Andmete konfidentsiaalsuse kadu. Ründajal on mobiiltöökohal võrdluses bürooruumidega oluliselt lihtsam juurde pääseda kõvakettal, ird- või paberkandjal olevatele andmetele. Samuti on võimalik pealt kuulata sideühendusi. Selliste andmete avalikustamisel või ründeks kasutamisel võivad olla organisatsioonile märkimisväärsed tagajärjed. Andmeleke võib kaasa tuua seaduserikkumise (näiteks isikuandmete paljastumise tõttu) või ebasoodsa konkurentsiolukorra. **Asutus rakendab Microsofti poolt soovitatud turbemeetmeid pilveteenuste turvaliseks kasutamiseks (nt mitmetasemeline autentimine jms).**

Kokkuvõte

Microsoft on teenusepakkujana rakendanud märkimisväärsed infoturbe ja andmekaitse alaseid meetmeid ning läbinud vastavad turbeauditid, millega saab lugeda teenusepakkuja usaldusväärseks. Samuti on Microsoftil andmete majutamise võimalus Euroopa Liidus, millega on formaalselt tagatud andmekaitsenõuete täitmine.

Microsoft klientidel (eriti avaliku sektori klientidel, kellel on võimalik sõlmida erilepinguid) on märkimisväärsed võimalused saada informatsiooni Microsoft toodete kohta ning seadistada Microsoft pilveteenuste kasutamine turvaliseks.

Samas on vajalik rakendada töökorralduslikke meetmeid, millega asutuse teenuste toimepidevus ei sõltuks ainult Microsoft pilveteenuste katkematust tööst (nt käitades osaliselt paralleelset taristut olulisemate funktsioonide dubleerimiseks *on-prem* keskkonnas).

Asutusel on võimalus teenusest koos andmetega igal ajal lahkuda ning jooksvalt teha varukoopiaid olulistest andmetest.

Eeltoodust tulenevalt on võimalik Microsoft pilveteenustes kasutada asutusesiseseks kasutamiseks mõeldud teavet.

Lisa 1. maatriks skooride arvutamiseks