Microsoft riskianalüüsi[1] lisa

Copilot AI

Kirjeldus

Käesolev riskianalüüs on Microsoft riskianalüüsi lisa ja keskendub Microsoft Copiloti AI pilvtöötlusteenuse (edaspidi Copilot) riskide kirjeldamisele ning ei kohaldu Microsoft toodetele, mida on võimalik kasutada asutuse sisestel ressurssidel. Tehisintellekti (artificial intelligence, AI) all mõistame mistahes süsteemi, mis suudab sooritada ülesandeid pealtnäha inimintelligentsi kasutades. Majandus- ja Kommunikatsiooniministeeriumi kratikavad on näinud ette tehisintellekti ulatuslikku rakendamist avalikus sektoris. LLMide (*large language model*) ning difusioonipõhiste pildisünteesimudelite levik ja tavatarbijale kättesaadavamaks muutumine on põhjustanud selles valdkonnas arenguhüppe, sealhulgas AIaaS (artificial intelligence as a service, tehisintellekt teenusena) ärimudeli leviku[2].

Copilot on Microsofti AI toode, mis on mõeldud kliendi toetamiseks ja aitamiseks. Copilot saab aidata klienti koodi kirjutamisel, sisu loomisel või teabe leidmisel. Copilot on integreeritud teiste Microsofti teenustega (Dynamics 365, Power Platform ja Microsoft 365).

Copilot kasutab LLM keelemudelit ning õpib ja kohaneb pidevalt päringutega mida talle esitatakse, pakkudes vastuseid. Copilot pakub juurdepääsu võimsale AI-le ja on üles ehitatud keelemudelile GPT-4 ja teksti pildiks muutmise mudelile DALL-E 3, mis on süvaõppemudel loomuliku keele kirjelduste põhjal digitaalsete piltide loomiseks, nii OpenAI-st kui ka mujalt. See põhineb Bingi otsinguindeksil, et pakkuda vastuseid kõige värskema teabe osas[3]. Copilot on loodud kooskõlas Microsofti AI põhimõtetega.

Copilotit saab kasutada ka avaliku veebiteenusena[4], mis on kõigile kasutajatele kättesaadav. Copilot on saadaval ka mobiilirakenduste Copilot, Bing, Edge, Microsoft Start ja Microsoft 365 kaudu. Microsoft volitatud töötlejate osas eraldi usaldusväärsuse hinnangut ei koostata ja usaldatakse teenusepakkujat.

Copiloti AI võimalused

Copilot pilveteenus (lisa 2) on ülemaailmselt kasutusel (enam kui 65 riigis), laia kasutajabaasiga ning tavakasutajale suunatud toodete kasutusele võtmine ei eelda kasutajatelt reeglina täiendavat väljaõpet. Microsoft 365 Copilot aitab muuta igapäevatööd produktiivsemaks, integreerides end Microsoft töövahenditesse nagu Word, Excel, PowerPoint, Outlook ja Teams. Tegemist on uue põlvkonna tehisintellekti (edaspidi AI) lahendusega, mis kasutab

[1] https://teenused.rit.ee/microsoft_pilveteenuse_riskianal%C3%BC%C3%BCs_2023.pdf
[2] Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf (ria.ee)
[3] Copilot Bingis: meie lähenemine vastutustundlikule teipimisele - Microsofti tugiteenus
[4] Copilot (microsoft.com)

LLM tehnoloogiat ja Microsoft Graph andmeid (kalender, e-mailid, vestlused, dokumendid, koosolekud jne.).

Asutused saavad kasutada Copilotit vastavalt vajadusele, kasvades või vähenedes vastavalt nõudlusele ja maksta ainult selle eest, mida nad tegelikult kasutavad. Kuna Copiloti tasu kujuneb litsentsipõhisest summast (vajab olemasolevat E3 või E5 litsentsi).

Copilot võimaldab juurde pääseda mis tahes interneti ühendust omavast seadmest. Copilot pilveteenust värskendatakse automaatselt uute funktsioonide ja veaparandustega, mis välistab vajaduse uuendusi käsitsi rakendada ja võimaluse, et kasutusel on aegunud tarkvara versioon.

Microsoft investeerib enda sõnul pidevalt pilveteenuste arengusse ja tootearendusse, pakkudes juurdepääsu uutele tehnoloogiatele ja funktsioonidele. See võimaldab kasutada täiustatud AI-d, analüütikat ja andmeid, et parandada teenuste pakkumist, tõhustada töövooge ja teha paremaid otsuseid.

Asutused saavad kiiremini käivitada uusi projekte, vähendada IT-infrastruktuuri haldamisega seotud koormust ja võimaldada töötajatel paindlikult ja turvaliselt töötada.

Copilotiga saad ligipääsu AI funktsioonidele, mis aitavad automatiseerida korduvaid ülesandeid, näiteks dokumendi kirjutamine Wordis, e-kirjade kokkuvõtete tegemine Outlookis, esitluse loomine PowerPointis, märkmete koostamine OneNote'is, visuaalsete aruannete loomine Excelis ja koosolekute ning tegevuste kokkuvõtmine Teamsi vestlustest ja koosolekutel.

Kogu Copiloti tegevus toimub MS Graphis kasutaja enda andmete sees ning andmeid\tulemeid ei kasutata AI õppeks ega lähe kuidagi teiste kasutajate andmetega kokku või segamini[5].

Copilot suudab teha kokkuvõtteid erinevatest Edge dokumentidest ja lehekülgedest[6]. Nimekirja formaatidest, millest Edge kaudu kokkuvõtteid teha saab täiendatakse jooksvalt. Kui Copiloti on asutuses lubatud, pääsevad kasutajad sellele ka ligi Edge'i mobiilirakenduse kaudu, kui nad on oma töökontoga (Entra ID) sisse loginud.

Copilot otsib veebist asjakohast sisu ja teeb seejärel kokkuvõtte leitud materjalist, et luua kasutajale vastus. Copilot viitab ka kasutatud allikatele, nii et kasutaja näeb lisaks vastustele ka kasutatud linke.

Skoor: võimaldab optimeerida baasteenuste kulusid ning maandab tarkvara uuendamisest tulenevaid turvariske– 2 (keskmine)

Copiloti AI puudused

Copiloti pilveteenuseid majutatakse väljaspool Eesti territooriumi ning vajavad üldiselt toimimiseks püsivat Interneti ühendust. Ühenduseta Copiloti pilve pikaajalise katkestuse korral on vajalik kasutada alternatiivseid rakendusi.

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[7].

Copilot kasutab LLM keelemudelit, mis jäljendab loomulikku inimkeelt treeningandmete põhjal. Mudel on optimeeritud vestluse jaoks, kasutades selleks inimeste tagasisidet

[5] https://learn.microsoft.com/en-gb/copilot/microsoft-365/microsoft-365-copilot-privacy

[6] Copilot in Edge webpage summarization behavior | Microsoft Learn

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

(*Reinforcement Learning with Human Feedback*).

Kui kasutaja teeb Copilotile pöördumise, genereerib mudel vastuse, tehes ettepanekuid sõnadereast, mis peaksid järgnema. Mudel põhineb domeenispetsiifilisel keelel (DSL), mis võimaldab täpsustada, millist teavet soovite otsida ja sünteesida Microsoft 365 andmetest. Kindlasti on oluline meeles pidada, et süsteem loodi loomuliku inimkommunikatsiooni jäljendamiseks, kuid väljund võib olla ebatäpne või vananenud. Kasutaja peaks võimalikult lihtsalt ja loomulikku keelt kasutades esitama Copilotile küsimusi. Samuti ka küsima lihtsalt sõnastades abi sisu loomisel või kokkuvõtte saamiseks dokumendist või vestlusest. Mida täpsem on kasutaja päring, seda paremad on vastused. Kuigi Copilot suudab paljudes olukordades aru saada, võib AI mõnikord segadusse minna keerukate või mitmetähenduslike lausete korral, nt kui küsitakse midagi väga spetsiifilist või ebatavalist, võib vastus olla ebatäpne. Kuna Copilot järgib ranget eetikakoodeksit, et mitte põhjustada kellelegi füüsilist, emotsionaalset või finantsilist kahju, võib mõnikord vastuste sisu olla piiratud[8].

Copilot on loodud pakkuma täpseid ja informatiivseid vastuseid, lähtudes teadmistest ja andmetest Microsofti Graph-is. Copilot kasutab Microsoft Graphi analüüsioskust, et sünteesida teavet dokumentidest, meilidest ja sõnumitest, mis võimaldab kokkuvõtete tegemist, küsimustele vastamist ja sisu loomist. Siiski ei pruugi vastused alati olla täpsed, kuna need genereeritakse keeleandmete mustrite ja tõenäosuste põhjal. Kahtluse korral tuleks alati kontrollida saadud teavet. Kvaliteedi tagamiseks esitatakse Copilotile testküsimusi ja saadud vastuseid hinnatakse täpsuse, asjakohasuse, tooni ja intelligentsuse alusel. Nimetatud hindamispunkte kasutatakse seejärel mudeli täiustamiseks.

Copilot on loodud imiteerima inimeste loomulikku suhtlust, kuid väljund võib olla ebatäpne, vale või aegunud. Kasutajad peaksid alati kontrollima oluliste faktide õigsust ja mitte täielikult usaldama Copiloti vastuseid. Lisaks võib olla Copiloti tõlge mõnikord ebatäpne või kohmakas. Tagasiside andmine aitab Copilotile õpetada, millised vastused on kasutajale kasulikud ja millised mitte, seda tagasisidet kasutab Microsoft Copiloti täiustamiseks. Copilot esitab ainult need andmed, millele igaüks ligi pääseb, kasutades samu juhtelemente andmetele juurdepääsuks, mida kasutatakse teistes Microsoft 365 teenustes.

Kui on kasutusel Copilot, võivad organisatsiooni ehk asutusesisesed andmed väljuda MS365 teenuse piiridest, järgmistel juhtudel:

- Kui on kasutusel pluginaid, mis aitavad Copilotil pakkuda asjakohasemat teavet. Tuleb kontrollida pluginate privaatsustingimusi ja kasutustingimusi, et teha kindlaks, kuidas organisatsiooni andmeid töötleb. Teavet leiab selle kohta Microsofti kodulehelt.
- Kui on kasutusel Copiloti vastuste täiustamiseks veebisisu pluginaid, genereerib Copilot otsingupäringu, mis saadetakse Bingile, et saada uuemat teavet veebist. Lisateavet selle osas leiab Microsofti kodulehelt[9].

Copilot võib töödelda tundlikke andmeid, mis võivad olla konfidentsiaalsed või sisaldada isikuandmeid. Selle riski maandamiseks jälgib Microsoft rangeid privaatsusstandardeid ning krüpteerib andmeid nii puhkeolekus kui ka edastamise käigus.

Copiloti pilve kasutamisel saab Microsoftist isikuandmete (all)volitatud või teine volitatud töötleja, kelle

[8] Microsoft Responsible AI Standard v2 General Requirements

[9] https://learn.microsoft.com/en-gb/copilot/microsoft-365/microsoft-365-copilot-privacy

andmekeskused paiknevad osaliselt USA-s ning Microsoftiga lepingut sõlmides ei ole võimalik kliendil oluliselt mõjutada lepingutingimusi.

AI süsteemi andmekaitsealastele nõuete tagamiseks peab võtma arvesse IKÜMi artikli 5 lõikes 1 kehtestatud isikuandmete töötlemise põhimõtteid, mille täitmise eest vastutab ja peab olema võimeline nõuete täitmist tõendama vastutav töötleja (IKÜM artikkel 5(2)).

USA-s tegutsevatele isikutele ja asutustele ja/või USA-s asuvatesse andmekeskustesse isikuandmete edastamine ei ole üldjuhul lubatud, sest Euroopa Liidu ja Ühendriikide vahel ei ole alates 2020. aasta juulikuust[10], 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*[11]), nagu kehtivad Euroopa Liidus toimuva andmetöötluse suhtes. Varasemad lepped EU ja USA vahel on korduvalt õigustühiseks tunnistatud. Töö uue vastava andmekaitseraamistiku loomise nimel käib siiski aktiivselt ja selle heakskiitmist võib prognoosida 2024. aasta jooksul. 2023 aastal vastu võetud *Data Privacy Frameworki* kohaldamise osas töö käib ja selle funktsionaalsust hinnatakse perioodiliselt (kontrollitakse, kas kõik asjakohased meetmed on rakendatud ning toimivad praktikas, et kaitsta isikuandmete edastamist EU-USA vahel).[12]

Skoor: tööprotsesside seisak, süsteemide funktsionaalsus andmete tervikluse ja salajasuse tagamine – 2 (keskmine)

Kasutajad ja asutused eelistavad Copiloti kasutusele võtmist, kuna pilverakendused pakuvad rohkem funktsionaalsust ning on kaasaegsemad. Copilot pakub kasutajatele võimalust koostada erinevaid kokkuvõtteid sisukatest ja pikkadest dokumentidest. Lisaks Copilot pakub kiirelt vastuseid tekkinud küsimustele ning võimaldab kasutajatel automatiseerida protsesse. Copilot võib aidata kasutajatel luua teksti, koodi ja muud sisu, mis võib vähendada tööaega ja suurendada tootlikkust. Kui asutus kasutab Copilotit arendusprojektides, võib see vähendada arendajate aega ja ressurssi koodi kirjutamiseks. See võib mõjutada arendusmeeskondade suurust või kulutusi. Asutused peavad investeerima koolitusse, et töötajad saaksid Copilotit tõhusalt kasutada. See võib hõlmata nii tehnilist moistmist. Copiloti kasutamine võib nõuda litsentsitasude maksmist Microsoftile. Copilot võib aidata vähendada vigade arvu koodis ja tekstis, mis võib omakorda vähendada paranduskulusid ja klientide rahulolematust. Copilotit saab kohandada vastavalt organisatsiooni vajadustele ning laiendada Microsoft Copilot Studio abil.

Copilot võib kasutajatele pakkuda mitmeid eeliseid ja mõjutada nende kogemust. Kuigi Copilot on võimas tööriist, peavad kasutajad olema teadlikud selle piirangutest ja järgima eetilisi suuniseid. Näiteks ei tohiks Copilotit kasutada konfidentsiaalsete andmete töötlemiseks. Copiloti kasutamine võib mõjutada kasutajate tööd, loovust ja suhtlemist, kuid see sõltub individuaalsetest vajadustest ja eesmärkidest.

Skoor: positiivne mõju protsessidele – 2 (keskmine)

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

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

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

Rahaline mõju

Microsoft 365 Business Standard/Business Premium klientidel on võimalik soetada Copilot Microsoft 365 - Microsoft Cloud solution Provider (CSP) partneri kaudu. Copiloti puhul on tegu nö lisatootega, mis nõuab lisaks põhitoodet (Microsoft 365 E3/E5, Office 365 E3/E5 või Microsoft 365 Business Standard/Business Premium). Lisatoote saab siduda olemasoleva põhitoote litsentsiga ja lõpukuupäeva saab valida põhitootega sama.

Copilot on saadaval sobiva litsentsiga kasutajatele:

- Microsoft 365 E3 või E5
- Microsoft 365 F1 või F3
- Microsoft 365 Business Standard, Premium või Basic
- Microsoft 365 rakendused ettevõttele või ettevõttele
- Office 365 E1, E1 Plus, E3, E5 või F3

Ettevõttelepingu (EA) kaudu ostetud Microsoft 365 E3 või E5 originaaltellimusega organisatsioonid ei pea enam kasutama Microsoft 365 E3 või E5 lisafunktsioonide litsentsi oma kasutajate jaoks Microsoft Copiloti haldamiseks.

Copiloti rahaline mõju sõltub asutusele sellest, kuidas seda kasutatakse, millistes valdkondades ja kui suures mahus. Asutused peaksid hindama oma konkreetseid vajadusi ja eesmärke, et teha teadlikke otsuseid Copiloti kasutamise osas.

AI tehnoloogiate rakendamine on tõusutrendis – selle turu suurus peaks 2027. aastaks ulatuma 407 miljardi dollarini. Ka Eesti ettevõtted kasutavad üha enam selliseid tehnoloogiaid – 2023. aasta I kvartali seisuga on olnud kasv 2% võrreldes 2021. aastaga. Statistikaameti andmetel kasutavad tehisaru tehnoloogiaid Eestis enim finants- ja kindlustus, info- ja side ning energeetika valdkonna ettevõtted[13].

Skoor: täiendav kulu eelarves – 3 (kõrge)

EL/NATO liikmesriigis hoitavad andmed

Microsoft peakontor asub USAs ja klientide andmete asukoht on kliendi enda valida, vaikimisi asuvad Eesti kasutajate andmed Euroopa Liidus. Andmeid on võimalik hoida erinevates regioonides. 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[14]).

Copilot järgib Microsofti toote- ja andmekaitsetingimustes kirjeldatud andmeresidentsuse nõudeid (Copilot lisati 01.03.2024). Alates 1. märts 2024. on Euroopa Liidu klientide jaoks Copilot MS365 *EU Data Boundary* teenus. Väljaspool Euroopa Liitu asuvate klientide päringuid võidakse töödelda USA-s, Euroopa Liidus või muudes piirkondades[15].

Andmete asukoht sõltub seega teenuse infrastruktuurist ja Microsofti serverite asukohtadest. Täpsemalt on kirjeldatud Microsofti riskianalüüsis.

[13] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

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

[15] https://learn.microsoft.com/en-gb/copilot/microsoft-365/microsoft-365-copilot-privacy

Skoor: võimalik valida, kus andmeid hoida – 2 (keskmine)

Vaikimisi säilitab Microsoft vestluste ajaloo andmeid 90 päeva alates vestluse viimasest värskendamisest.

Vestluse ajaloo kustutamine on kasutaja jaoks tehtud lihtsaks ning võimaldab kasutajal kogu vestluse ajaloo kiirelt kustutada. Lisaks on võimalik kasutajal teenuse kasutamisel valida salvestamise välja lülitamise, mis takistab kasutaja otsinguajaloo salvestamist[16]. Kui asutusesiseste andmete kaitse on lubatud, ei toeta Copilot vestlusajaloo funktsiooni, mis ei säilita vestlusjuhiseid ega vastuseid.

Andmete säilitamise aeg sõltub teenuse seadistustest ja Microsofti poliitikatest. Andmeid töödeldakse ja säilitatakse vastavalt teenuse kasutamisele ning vajadusele.

Andmekao vältimiseks peaks andmete omanik hindama Copiloti pilveteenuses olevat andmete koosseisu ning nende ajaloolist väärtust, et hinnata, kas andmete eksportimine on vajalik ja otstarbekas.

Skoor: võimalik teenusest lahkuda ja eksportida andmeid – 2 (keskmine)

Vastavus sertifikaatidele ja nõuetele (ISO, E-ITS jms)

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid[17]. Microsofti riskianalüüsis väljatoodud sertifikaadid on vastavuses ka Copilot AI pilvteenusega. Täiendavaid sertifikaate Copiloti osas ei ole teadaolevalt. AI juurutamisel tuleks lähtuda juhtimissüsteemi rakendamisest, nt ISO/IEC 42001, mida saaks integreerida vajadusel ISO 9001 ja ISO/IEC 27001 standarditel põhineva juhtimissüsteemidega. Asutused saavad AI kasutuselevõtu korral lähtuda olemasolevatest infoturbe ja andmekaitse vastavusnõuetest.

Küberturvalisusel on oluline roll, et tagada AI süsteemide vastupidavus katsetele muuta nende kasutamist, käitumist, jõudlust või ohustada turvaomadusi pahatahtlike kolmandate osapoolte poolt, kes võivad süsteemi haavatavusi ära kasutada. Ründajad võivad võtta sihikule nt treeningandmed (andmemürgitus), treenitud mudelid (pahatahtlik rünne või kuuluvuse tuvastamise rünne) või kasutada ära AI süsteemi digitaalsete varade või selle aluseks oleva IKT infrastruktuuri haavatavusi. Riskidele vastava küberturvalisuse tagamiseks tuleb rakendada sobivaid ja tõhusaid meetmeid, võttes arvesse ka praegust tehnoloogia taset.
Euroopa Komisjon avalikustas 2021. aasta aprillis esimese AI-d reguleeriva raamistiku. Viidatud ettepanek on kantud riskipõhisest lähenemisviisist ehk AI süsteeme tuleb analüüsida ja klassifitseerida vastavalt sellele, millist ohtu need kasutajatele kujutavad. Samas ei tohi ära unustada ka kehtivat õigusraamistikku[18].

13. märts 2024 vastuvõetud AI määrus sätestab tingimused, millistel juhtudel on AI süsteemi kasutamine keelatud, nt kui see põhjustab kahju inimese elule, tervisele või põhjustab diskrimineerimist (artikkel 5)[19]. AI määrus kirjeldab ka, millised on riskitasemed AI süsteemide osas ning reguleerib ka AI süsteemide kasutamist ja

[16] Sinu igapäevane tehisintellekti kaaslane | Microsoft Bing

[17] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

[18] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

[19] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

määratleb rikkumisest teavitamise võimalused (nt järelevalveasutuse).

Kui AI süsteem või seda opereeriv isik kuulub määrus(t)e kohaldamisalasse, tuleb hinnata, millised konkreetsed nõuded määrus(te)st tulenevad GDPR-i kohaselt on oluline hinnata, kas kvalifitseerutakse näiteks isikuandmete vastutavaks või volitatud töötlejaks, AI määruse puhul aga näiteks AI-süsteemi teenustajaks (”provider”) või juurutajaks (”deployer”). Määruste kohaseid rolle on veelgi ja ka need on mõistlik üle vaadata. Konkreetsete nõuete tuvastamiseks on vaja teada ka seda, mis on andmetöötluse ja AI kasutamise eesmärk, millised andmetöötlusprotsessid süsteemis toimuvad, millised andmed ja kelle vahel liiguvad ning millist AI-süsteemi või komponenti (sh selle riskitase) süsteemis kasutatakse[20].

Standardite järgimine panustab toodete või teenuste ohutuse, kvaliteedi ja töökindluse tagamisse, samuti võivad need parandada ja tõhustada ettevõtte süsteeme või protsesse. AI süsteemide erinevate elutsüklite puhul rakendatavate standardite kohta on võimalik lugeda ENISA publikatsioonist heade küberturvalisuse praktikate kohta AI süsteemide puhul[21]. Täpsemalt on kirjeldatud Microsofti riskianalüüsis.

Skoor: olemasolevad sertifikaadid on vastavuses KüTS nõuetega – 1 (madal)

Andmekaitse meetmete rakendamine

Copilot rakendab rangeid privaatsuse ja turvapõhimõtteid, et kaitsta sinu andmeid ja järgida standardeid. Copiloti privaatsuse ja turvalisuse põhifunktsioonide kohaselt:

- Copilot ei jaga sinu andmeid kolmanda osapoolega, välja arvatud juhul, kui oled ise selleks loa andnud.
- Copilot ei kasuta sinu andmeid kolmandate osapoolte toodete või teenuste treenimiseks ega parendamiseks, näiteks OpenAI puhul.
- Copilot ei kasuta sinu andmeid Microsofti AI mudelite treenimiseks ega parendamiseks, väljaarvatud kui sinu ettevõtte administraator on valinud valikulise andmete jagamise.
- Copilot järgib olemasolevaid andmekaitse regulatsioone ja -poliitikaid ning kasutajad näevad ainult vastuseid, mis põhinevad nendele juurdepääsetavatel andmetel.
- Copilot krüpteerib andmeid nii puhkeolekus kui ka edastamise käigus, tagades tugevad turvameetmed.
- Copilot blokeerib päringusisestused (*jailbreak*-rünnakud), mis on mõeldud AI mudelit provotseerima soovimatute käitumiste näitamiseks.

Copilot järgib mitmeid eetikakoodekseid, et tagada vastutustundlik ja ohutu suhtlus. Copilot ei avalda isiklikku teavet ega riku privaatsust, mis hõlmab nimesid, aadresse, sotsiaalkindlustuse numbreid ja muid isikuandmeid. Copilot ei tohi pakkuda teavet, mis võiks kellelegi füüsilist, emotsionaalset või finantsilist kahju tekitada, mis hõlmab ohtlikke nõuannete andmist, ebaseaduslikke tegevusi või muud riskantset sisu. Copilot ei tohi luua sisu, mis diskrimineerib inimesi nende rassi, soo, seksuaalse sättumuse, usutunnistus või muude isiklike omaduste alusel. Kui Copilot satub eetilisse vastuollu, järgib ta ettevaatlikkust ja konservatiivsust, nt kui küsitakse midagi ebasobivat, keeldub

[20] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

[21] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

Copilot sellele vastamast või pakub neutraalset teavet.

Copilot järgib olemasolevaid privaatsuse, turvalisuse ja vastavuskohustusi, sealhulgas isikuandmete kaitse üldmäärust (GDPR) ja Euroopa Liidu (EL) andme edastuse piiranguid. Isikuandmete kaitse üldmäärus peab oluliseks kaitsta füüsilisi isikuid isikuandmete automatiseeritud töötlemise puhul. Lisaks eelnevale peab tehisaru arendamisel, rakendamisel ja kasutamisel arvestama ka muude nõuetega, näiteks intellektuaalomandi õigusega.

Skoor: andmekaitsetingimused on täidetud – 2 (keskmine)

Andmekaitsetingimused

Vastuste koostamisel kasutab Copilot töötlemiseks globaalseid andmekeskusi ja võib andmeid töödelda Ameerika Ühendriikides. Valikulised Bingi toega ühendatud teenused ei kuulu Microsofti EU Data Boundary (EUDB) kohustuste alla. Need ei kuulu ka andmekaitse lisa (DPA) tingimuste alla, mis nõuab, et ettevõtte andmed jääksid geograafiliste või tenantite piiridesse.

Organisatsioonid, kellel on ranged nõuded, et andmed peavad jääma tenantite või geograafiliste piiride piiresse, peaksid generatiivsete AI-teenuste pakkumiseks kaaluma hoopis Microsoft 365 jaoks mõeldud Copiloti või Azure Open AI kasutamist. Kaubandusliku andmekaitsega Copilot on mõeldud organisatsioonidele turvalisema alternatiivina kui tarbijale suunatud generatiivsete AI-teenuste kasutamine. Sellest tulenevalt on võimalik kliendil tutvuda meetmetega ning veenduda, kas need on piisavad andmekaitse tagamiseks.

Copiloti kasutamisele kohaldatakse ka Microsofti privaatsustingimusi, mis kirjeldavad Copiloti kasutamisega seotud teabe kogumist, kasutamist ja avaldamist. Nii kasutaja kui ka organisatsiooniandmed on kaitstud, viibad (*prompts*) ja vastuseid ei salvestata, Microsoftil ei ole otsest juurdepääsu ja vestlusandmeid ei kasutata keelemudelite koolitamiseks. LLMidel põhinevate vestlusrobotite viibale liidetakse ka eelviip (*pre-prompt*) mis sisaldab täiendavat infot vestluse konteksti, kasutaja ning ka keelemudeli kohta. See on oluline muuseas selleks, et juturobot lähtuks väljundis oma rollist juturobotina, kes vastab küsimustele, selle asemel et genereerida jätku kasutaja sisendile. Eelviibaga saab kaasa anda teavet välismaailma kohta, näiteks kuupäeva, kellaaja, kasutajanime, dokumendi või tekstifaili sisu või muid kasutaja või keskkonna tunnuseid. Mudelid ei suuda eristada viipa eelviibast, ning see on asjaolu, mida kasutavad ära paljud viibasüstimise tehnikad. Et eelviipa on oskusliku viipamisega võimalik kasutajal kergesti pärida, ei tohi see kanda infot, millele kasutajal ei tohiks ligipääsu olla[22].

Erinevalt Microsoft 365 Copilot versioonist ei ole Copilotil juurdepääsu Microsoft 365 organisatsiooni sisestele andmetele[23].

Kui organisatsioonid ja kasutajad kasutavad generatiivseid AI-teenuseid, on oluline mõista, kuidas need teenused kasutaja- ja vestlusandmeid töötlevad. Töötajate vestlused võivad sisaldada tundlikke andmeid. Copiloti sisestatud ja sealt saadetud vestlusandmed krüpteeritakse edastamisel *Transport Layer* turvaprotokolli (TLS 1.2+) abil ja puhkeolekus täiustatud krüpteerimisstandardi (AES-128) abil. Microsoftil pole nendele andmetele otsest juurdepääsu.

Copilot pääseb läbi vestluse organisatsiooni andmetele juurde ainult

[22] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

[23] Overview of Copilot | Microsoft Learn

siis, kui kasutajad seda aktiivselt ise sisestavad. Andmeid esitatakse Copilotile vastavalt kasutaja juurdepääsuõigusest, mis tähendab, et Copilot ei saa juurdepääsu konfidentsiaalsetele andmetele, millele kasutajal õigust pole. Kasutajad saavad lubada Copilotil oma organisatsiooni andmetele juurde pääseda kolmel viisil:

- Kasutajad sisestavad või kleebivad selle teabe otse vestlusesse.
- Kasutajad laadivad faili üles, valides vestluskasti vasakus alanurgas kirjaklambriikooni. Samuti saavad nad faili vestluskasti tõsta.
- Pärast sätte valimist „Luba juurdepääs mis tahes veebilehele või PDF-ile" korral võib Copilot kasutada seda sisu küsimustele vastamiseks.

Kõigil juhtudel, kui andmed on lubatud, ei säilita Copilot neid andmeid pärast vestlusseansi lõppu. Samuti ei kasutata organisatsiooni andmeid keelemudeli koolitamiseks[24].

Kui kasutaja suhtleb Copilotiga, mis on ühendatud Microsoft 365 rakendustega (nt Word, PowerPoint, Excel, OneNote, Loop või Whiteboard), salvestab Microsoft nende tegevuste osas andmeid. Salvestatud andmed sisaldavad kasutaja viipa ja Copiloti vastust, sh tsitaate mis tahes teabele, mida kasutatakse Copiloti vastuse koostamiseks. Näiteks on need salvestatud andmed kasutajate Copiloti interaktsiooni ajalugu koos graafikupõhise vestluse ja koosolekutega Microsoft Teamsis. Neid andmeid töödeldakse ja salvestatakse kooskõlas organisatsiooni ja Microsofti vahelise lepinguliste kohustuste täitmisega. Andmed krüpteeritakse nende säilitamise ajal ja neid ei kasutata LLM-ide koolitamiseks, sh neid andmeid, mida kasutab Copilot Microsoft 365.

Salvestatud andmete vaatamiseks ja haldamiseks saavad administraatorid kasutada sisuotsingut või Microsoft Purview't. Administraatorid saavad kasutada ka Microsoft Purview't Copilotiga vestlusega seotud andmete säilitamise reeglite/poliitikate määramiseks[25].

Skoor: andmekaitse tagamine on kooskõlas määrusega – 2 (keskmine)

Turvameetmete rakendamine

Microsofti poolt rakendatavad turvameetmed kohalduvad ka Copilot AI pilveteenusele.

Kasutajad peavad kasutama Copilotit ja loodud loomingut ainult seaduslikult ja kooskõlas kõigi kohaldatavate seadustega; vastavalt Microsoftiga sõlmitud lepingule, sisupoliitikale ja Microsofti teenuste dokumentatsioonile; ja viisil, mis ei riku ega püüa rikkuda, omastada või muul viisil rikkuda ühegi teise isiku või üksuse õigusi. Käitumiskoodeksi ja/või sisueeskirjade tõsine või korduv rikkumine võib kaasa tuua kasutajale Copiloti kasutamise peatamise[26]. Kasutaja saab Copiloti peatamise peale edasi kaevata, esitades kaebuse vastava kasutajaliidese kaudu. Microsoft jätab endale õiguse Copiloti kasutamine jäädavalt peatada[27].

Microsoft on kehtestanud põhimõtted, mis juhivad AI vastutustundlikku arendamist ja kasutamist. Need põhimõtted hõlmavad õiglust, usaldusväärsust ja ohutust, privaatsust ja turvalisust, kaasatust, läbipaistvust ja vastutust. Microsofti lähenemine AI-le on inimkeskne, loodud selleks, et suurendada inimeste võimeid ja lähtuda eetilistest kaalutlustest, mis on

[24] Copilot Privacy and Protections | Microsoft Learn
[25] https://learn.microsoft.com/en-gb/copilot/microsoft-365/microsoft-365-copilot-privacy
[26] Microsofti teenuselepe
[27] Terms of use | Microsoft Learn

sügavalt juurdunud püsivates väärtustes ja inimõigustes.

Copilot krüpteerib andmeid nii puhkeolekus kui ka edastamise käigus, tagades turvameetmed, mis kaitseb andmeid volitamata juurdepääsu eest.

Microsoft kasutab teenuste kaitsmiseks küberohtude eest mitmeid meetodeid, sh:

- AI toega ohutuvastust, et märgata muutusi võrgu ressurssides või -liikluses;
- käitumisanalüütikat riskantsete sisselogimiste ja anomaalse käitumise tuvastamiseks;
- masinõppemudelid riskantse sisselogimise ja pahavara tuvastamiseks;
- Zero Trusti, kus iga juurdepääsutaotlus peab olema täielikult autenditud, volitatud ja krüptitud;
- ja kontrollib seadme tervist enne, kui seade saab ettevõtte võrguga ühenduse luua[28].

Microsoftil on AI punane meeskond (*red team*), kes tegeleb vigade ja nõrkuste tuvastamisega selleks, et saaks küberrünnakuid ennetada[29].

Skoor: rakendatud turvameetmed muudavad teenuse kasutamise ohutumaks – 2 (keskmine)

Riskid

AI-ga seotud riskid	Andmete töötlemise osas pole võimalik veenduda, kuidas ja milliseid andmeid töödeldakse ning mis otsuseid AI teha võib andmete pinnalt. Andmete lekkimise oht (konfidentsiaalsed- ja isikuandmed). **Kindlad protseduurid, milliseid andmeid antakse ning millised on reeglid töötlemisel. Tehakse konkreetsele pakkujale/tehnoloogiale turvaanalüüs seoste/tagauste tuvastamiseks ja võetakse tootepõhiselt kasutusele lisaturvameetmeid.**
	Andmete töötlemisel ei saa tagada, et järgitakse GDPR-i. AI võib valimatult koguda andmeid, mille õiguslikku alust töötlemiseks pole. AI võib andmeid muuta selliselt, et tekib kahju asutusele. Kuna töödeldakse näiteks pöördumiste sisu on pahatahtlikul muutmisel suur mõju IT-abile ja kasutajale. **Andmed anonümiseerida või muuta isikustamata kujule. Majutada enda juures. AI kasutuselevõtu korral tuleb veenduda, et asutuse osas antud info väljund ei oleks asutuse mainet kahjustav.**
	Ründajad kasutavad ära AI turvanõrkusi, et saada ligi kasutajate andmetele. AI mitte otstarbelisest kasutamisest võib tekkida turvanõrkus. AI-d kasutatakse küberrünnakuteks, et pääseda mööda turvanõuetest ja seeläbi ära kasutada süsteeme. **Erinevate tarkvarade kasutuselevõtmine, mis kaitseb kahjurprogrammide eest. AI süsteemid ei tohiks määratletud tingimustel viia olukorrani, kus inimelu, tervis, vara või keskkond on ohus.**
	AI teadlikkuse kasv ning õppimisvõime muudab AI-d autonoomsemaks ning AI võib võtta vastu otsuseid, mis ei ole kooskõlas tellija nõuetega. AI võib teha otsuseid iseseisvalt, mis tekitab täiendavat turvariski. Andmete lekke ning andmete väärkasutamise oht suureneb. **AI määruse vastuvõtmine EU poolt, täiendavate kriteeriumite loomine ja järgimine, mis alustel tohib AI-d kasutada.**

[28] Cyber Signals: How Microsoft protects AI platforms against cyberthreats | Microsoft Security Blog

[29] Microsoft AI Red Team building future of safer AI | Microsoft Security Blog

AI-ga seotud riskid	Intellektuaalse omandi osas rikkumine, kui pole selge, kellele vastutus kuulub. Kiired regulatiivsed muudatused võivad kaasa tuua keelde AI kasutuselevõtu osas või liigselt piirata turgu, mistõttu võivad olemasolevad lahendused olla keelatud ning vastuolus seadusega. **Pidev arengute järgimine, et käia kaasas kehtiva seadusandlusega ning anda ka sisendeid seaduse muudatuste osas (õigusloomesse panustada riigi tasandil).**
	AI on soodsam kui inimtööjõud. AI otsuseid on vaja kontrollida ja on vaja inimressurssi, et õpetada AI-d. Ainult AI-st sõltumine tekitab täiendavat riski. Kuna AI areneb, siis on vaja kvalifitseeritud tööjõudu, kes suudaks AI-d arendada ja kontrollida. Ilma kvalifitseeritud tööjõuta ei suudeta kasutada AI kogu potentsiaali ning võidakse teha vigu. **Tööprotsesside seadmine selliselt, et ainult AI otsuste pinnalt ei tehta otsuseid, ning neid otsuseid valideerib viimasena inimressurss. Oskusjõud valideerida ja jälgida AI kvaliteedimõõdikuid ning vajadusel neid peen häälestada.**
	AI sooritatud tegevuste ning langetatud otsuste eest vastutab AI treener, kes teda õpetas. Kui AI hakkab asutuse mainet kahjustama ning konfidentsiaalseid andmeid jagama, siis vastutab töötaja, kes AI-d õpetas. **Personali ressurss, et palgata AI-d tundvaid töötajaid. Vastutustundlik projekteerimine, arendus ja kasutuselevõtt, juurutajatele selge teave süsteemi vastutustundliku kasutamise kohta, juurutajate ja lõppkasutajate vastutustundlik otsuste tegemine, riskide selgitused ja dokumenteerimine, mis põhinevad juhtumite empiirilistel tõenditel.**
	Raske on tuvastada või parandada AI vigu või nõrkusi, mis ei ole hästi defineeritud või üheselt mõistetavad. Puudub vastav kompetents, kes suudaks vigu kiirelt märgata ning neid ennetada. **Personali ressurss, et palgata AI-d tundvaid töötajaid. Lisada inimkontroll, kui AI ei suuda ise vigu tuvastada või parandada. Teostada testimisi ning monitooringut. Domeenisisene testimine, reaalajas jälgimine ja võimalus sulgeda, muuta või lasta inimesel sekkuda süsteemidesse, mis erinevad kavandatud või oodatud funktsionaalsusest.**
	AI-st sõltumise korral lähtutakse ainult AI toest ja selle puudumisel protsessid pidurduvad. Tekitab loovuse puudujääke ning vähenevad inimkompetentsid. Riski põhjustab asjaolu, et AI sooritab tegevusi ning teeb otsuseid teisiti kui inimene. **Alternatiivide omamine, et ei sõltuks ainult AI-st ja oleks võimalik vajadusel ka valideerida AI poolt tehtavat. Kvaliteedimõõdikute paika panemine ja jälgimine, mis võimaldab järjepidevalt mõõta AI sisulist toimimist ning anda alust tema peenhäälestamiseks.**
	Andmete kustutamises ei saa veenduda, kuna konto üleminekul on võimalik kontol olev andmestik kolmandale isikule edasi anda (nt juhile). Ei saa kontrollida, kas andmed on kustutatud. **Sätestada asutusesisene protseduur andmete kustutamise osas.**
	Kasutajate tehtud vead ja eksimused, mille läbi antakse AI-le töötlemiseks konfidentsiaalset teavet ning isikuandmeid. Sisestatakse andmeid, mis kahjustavad asutuse mainet ning tekitavad turvanõrkusi (võrgujoonised, riskid, protsesside kirjeldused jms). **Rakendada asutusesisesed protsessid ja poliitikad, mille kaudu kasutajal pole võimalik vastavaid andmeid sisestada. Koolitada kasutajaid ning koostada vastavaid juhendeid, kuidas AI-ga tööd teha. Privaatsuse tagamiseks tuleb rakendada asjakohast andmehaldust (nt pääsuprotokolle) ja koostada andmekaitsealane mõjuhinnang.**

Kokkuvõte

Microsoft Copilot on rakendanud rohkeid infoturbe ja andmekaitse alaseid meetmeid, millega saab lugeda teenus usaldusväärseks. Samuti on Copilotil andmete majutamise võimalus Euroopa Liidus, millega on formaalselt tagatud andmekaitsenõuete täitmine.

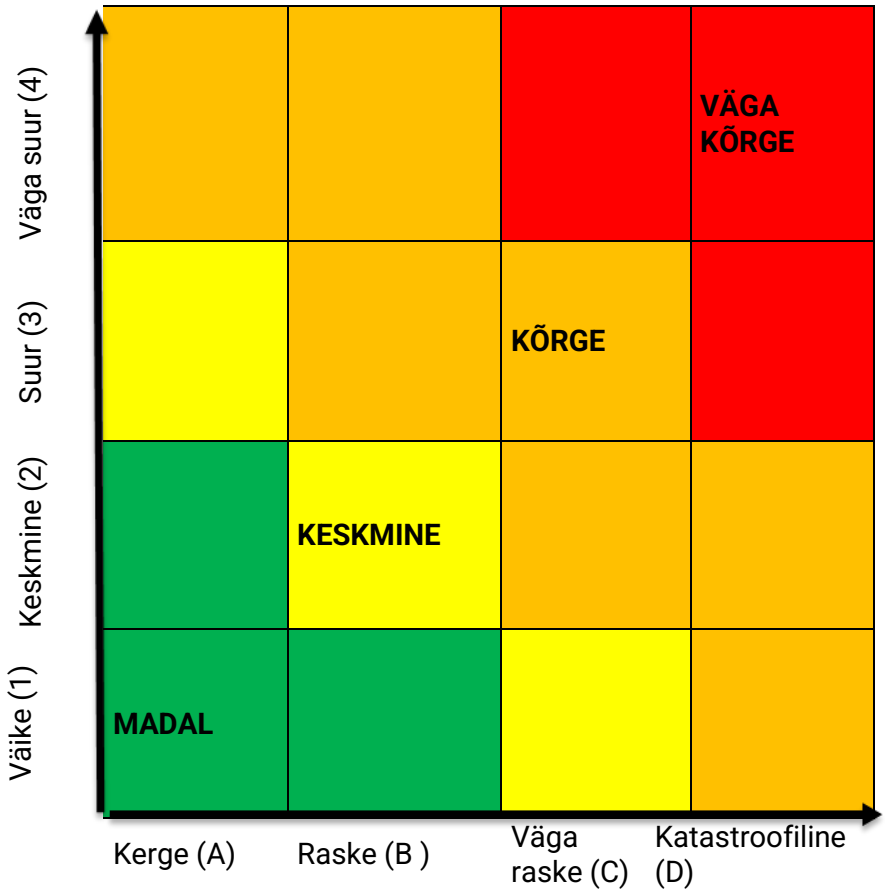
Copilot pakub klientidele rohkeid võimalusi, kuidas muuta kasutajate töö produktiivsemaks ja kulutõhusamaks. Copilot klientidel on võimalus seadistada Copiloti pilveteenuse kasutamine turvaliseks. Samas on vajalik rakendada täiendavaid töökorralduslikke meetmeid ning luua asutusesiseseid protsesse, millega on tagatud turvaline AI kasutamine.

Lisaks tuleb tagada, et asutuse teenuste toimepidevus ei sõltuks ainult Copiloti teenuse katkematust tööst.

Tulenevalt eelnevast ei saa olla lõpuni veendunud, kas Copilot on sobiv asutusesiseseks kasutamiseks mõeldud teabe töötlemiseks. Vajalik on rakendada täiendavaid meetmeid paralleelselt Copiloti kasutamisega, mh koolitada kasutajaid, alternatiivsete töömeetodite arendamine, Copilotile kätte saadavate andmete kontrollimine jms.

Arvestades, et AI kasutamise reguleerimine EU tasandil on alles algusfaasis, siis ei saa soovitada Copilot pilveteenuse kasutamist asutusesiseseks kasutamiseks mõeldud teabe töötlemiseks, kuni pole vastavaid regulatsioone kohalikul tasandil kehtestatud.

Lisa 1. maatriks skooride arvutamiseks



Lisa 2. Copilot AI joonis