Gemini

Kirjeldus

Käesolev usaldusväärsuse hinnang keskendub Google LLC pilvtöötlusteenuse (edaspidi Gemini) riskide kirjeldamisele ning ei kohaldu Google LLC 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.

Google on pilvteenuste ja tehisaru tehnoloogiate pioneer, üks maailma suurimaid ettevõtteid ning ühtlasi ka tuntumaid ja väärtuslikumaid brände[1] [2].

Tehisaru vestlusrobotitele suunduvast veebiliiklusest hõivab Google Gemini ligikaudu 3%, turuliider on OpenAI umbes 80%-ga[3].

Erinevate parameetrite põhjalt koostatud järjestustabelites, mis hindavad suurte keelemudelite kvalitatiivseid ja kvantitatiivseid võimeid, jäävad Gemini mudelid turuliidrile OpenAI'le enamasti mõnevõrra alla[4] [5].

Tehisaru vestlusrobotite arendajate seas on Google suurima taristuvõimega ettevõte: Google Cloud Computing, millel töötavad kõik Google'i pilvteenused, on Amazon Web Services'i ja Microsoft Azure'i järel suuruselt kolmas pilvtöötlusteenustaja maailmas[6].

Tugev majasisene taristuvõime, lai pilvteenuste spekter ning suur turuosa paljudes pilvteenuste valdkondades annab Google'ile suhteliselt hea positsiooni oma keelemudelite ja tehisaru vestlusroboti teenuse arendamiseks ning integreerimiseks teiste teenustega[7].

Ettevõtte suur tulubaas võimaldab subsideerida tehisaru tehnoloogiate arendamist ja turustamist pikema aja vältel ilma, et oleks tarvidust kaasata kapitali väljastpoolt. Toodud asjaolud on ettevõtte eeliseks sarnaseid tehisaru teenuseid arendavate ja turustavate konkurentide ees (OpenAI, Anthropic, Perplexity, Mistral jt}, kelle jaoks on tehisaru keskne ärisuund ning kelle jätkusuutlikkust mõjutavad nii teenuste turustamise kui ka kapitali

[1] https://companiesmarketcap.com/
[2] https://www.kantar.com/Campaigns/BrandZ/Global
[3] https://gs.statcounter.com/ai-chatbot-market-share
[4] https://artificialanalysis.ai/leaderboards/models
[5] https://www.vellum.ai/llm-leaderboard
[6] https://www.srgresearch.com/articles/q2-cloud-market-nears-100-billion-milestone-and-its-still-growing-by-25-year-over-year
[7] https://www.tomsguide.com/ai/forget-chatgpt-gemini-looks-set-to-win-the-ai-race-heres-why

kaasamise edukus üha suuremaid mullistusi kogeval AI-turul[8].

Gemini on ulatusliku teabekorpuse põhjalt masinõppe meetoditega treenitud keelemudelitel (LLM) töötav tehisaru vestlusrobot ja virtuaalne assistent, millega saab kasutaja suhelda loomulikus inimkeeles.

Organisatsioonidele on Gemini mudelid kasutatavad eri vormides ja eraldi teenustena:

1. ühe teenusena organisatsioonidele mõeldud kobarteenuse paketis Workspace[9];
2. organisatsioonidele mõeldud tehisintellekti tööriistade täiskomplekti teenuses Gemini Enterprise (lansseeriti 9. oktoobril 2025).
3. rakendusliidese (AP/) kaudu[10].

Käesolev usaldusväärsuse hinnang käsitleb neist esimest. Teenustaja tõi Gemini Enterprise paketi turule alles oktoobris 2025, mistõttu käesolev hinnang sellele ei keskendu.

Gemini volitatud töötlejate osas eraldi usaldusväärsuse hinnangut ei koostata ja usaldatakse teenusepakkujat.

Teenuse võimalused

- Genereerib ideid.
- Koostab loome- ja tarbetekste (luuletusi, jutustusi, reklaamtekste, juhendeid, teabelehti jms).
- Otsib Internetist teavet ja annab viited.
- Suudab tõlgendada ja kirjeldada etteantud pildimaterjali (sh diagramme ja tehnilisi jooniseid).
- Loob etteantud kirjelduse järgi pilte ja videoklippe.
- Loeb ja koostab faile levinud dokumendivormingutes (.txt, .docx, .xlsx, .ppt, .pdf jt}.
- Loeb ja koostab koodi erinevates programmeerimiskeeltes.
- Koostab põhjalikke referaate ja ülevaateid etteantud teemal ning paljude teabeallikate põhjal.

Ülaltoodud võimete realiseerimise võimalus ja kvaliteet sõltub sellest, millist keelemudelit kasutaja käsu täitmiseks rakendab. Keelemudelid, mida Gemini pakub, on[11]:

- Gemini 2.5 Flash-Lite;
- Gemini 2.5 Flash;
- Gemini 2,5 Pro.

Pakutavad mudelid paiknevad skaalal: kiirem, ent veaaltim (sobib lihtsatele küsimustele vastamiseks) vs aeglasem, ent analüütilisem ja faktitäpsem (sobib keerukamate probleemidele lahenduse otsimiseks).

Mistahes keelemudeli taustal töötavad ka graafilist väljundit loovad mudelid, mis käivituvad vastava korralduse peale vestluses:

- Gemini 2.5 Flash Image - redigeerib ja loob uusi kujutisi ette antud kujutiste põhjal;
- Imagen 4 - loob kirjelduse põhjal kujutisi;
- Vea 3.1 - loob kirjelduse põhjal videoklippe.

NB! Juurdepääsu Gemini mudelitele rakendusliidese (AP/) kaudu pakub Google eraldi teenusena, mistõttu käesolev hinnang seda ei käsitle.

SaaS - olemuselt on Gemini teenustaja pilvetaristul vestlusroboti vormis töötav virtuaalne assistent, mida saab kasutada:

- veebisirvija kaudu veebilehel;
- mobiilseadmete rakendustes (iOS ja Android);

[8]https://teadus.postimees.ee/8349598/new-scientist-tehisaru-mull-on-lohkemas-kuid-see-ei-tahenda-veel-tehisintellekti-surma

[9]https://workspace.google.com
[10]https://ai.google.dev/gemini-api/docs/pricing
[11]https://ai.google.dev/gemini-api/docs/models

- pistikrakenduses Google Chrome'i veebisirvijal (pakutakse hetkel vaid eraklientidele mõeldud pakettides).

Nende suhtluskanalite kaudu kättesaadavat teenust nimetab teenustaja koondnimega Gemini Apps[12].

Gemini vestlusrobot annab vastuseid kasutaja esitatud sisendinfo ja korralduste ajel üksikute käsundite (promptide) kaupa. Geminit iseloomustavad erinevad üldvõimed.

- „Saab aru" kasutaja tekstist (nii kirja- kui ka kõnekeelsest), selles sisalduvatest abstraktsematest mõtetest, konkreetsetest väidetest ja korraldustest.
- „Saab aru" ja vastab eri keeltes, kuid vastuste sõnavara ja süntaksi kvaliteet varieerub keeleti, sõltudes keelemudeli treenimisel kasutatud konkreetse keele korpuse mahust.
- Vastab sidusas ja korrektses keeles, liigendab ja vormindab vastustekstid lugejale hõlpsasti loetavaks.
- Arvestab vastustes sama vestluse varasemat konteksti.
- Sõnastab vastused kasutaja soovidest lähtuva tonaalsuse, sõnavaralise keerukuse ja üldistusastmega.
- Vestleb kasutajaga nii kirjalikus kui ka suulises vormis (mobiilirakenduses).
- Talletab varasemad vestlused arhiivi ja võimaldab neid igal ajal jätkata.
- Võimaldab luua rätsepkohaldusega juturoboteid (nn Gem-e), mis vestlevad ja täidavad korraldusi kasutaja määratletud eeskirjade raames ning kasutaja antud teabe põhjalt ja kontekstis.
- ühendub kasutaja (administraatori) volitusel mõnede Google Workspace'i teenustega, et töödelda kasutaja korralduse alusel neis sialduvaid andmekogumeid (märkmeid, kalendrisissekandeid, e-kirju, tekstidokumente, pilte, programmikoodi jm); hetkel ühendub Gmaili, Drive'i, Calendari, Keepi ja Tasksi teenustega[13] [14].

Gemini spetsiifilised võimed.

- Töötleb etteantud tekste nii tehniliselt kui ka sisuliselt: otsib välja ja tõstab esile spetsiifilisi sümboleid või sisupunkte, teeb sisukokkuvõtteid, pakub parandusi ja viib need sisse.
- Lahendab loogika-, arvutus- ja analüütikaülesandeid ning selgitab, kuidas tulemuseni jõuti. Pakub kaalutlevaid vastuseid filosoofilistele ja eetilistele küsimustele.

Teenustajal on olemas teenuse staatuse lehekülg, kus antakse ülevaade kõikide Google Workspace'i komplekti kuuluvate pilvteenuste hetkeseisust ning rikkesündmuste ajaloost koos kirjelduste ja täpsete kellaaegadega, mil rike aset leidis[15].

Google Workspace'i avalikus teenusetasemelepingus võtab Google kohustuse tagada kogu teenuskomplekti aktiivaeg (uptime) vähemalt 99,9%-l ajast igas kalendrikuus[16].

Kuna teenustaja kogeb praegu ja eeldab ka lähitulevikus Gemini kasutajate arvu väga kiiret kasvu, siis nenditakse, et ei suudeta kogu aeg tagada Gemini maksimaalset käideldavust ja töökiirust ning mõnikord tuleb klientidel rakenduse kasutamise käigus kogeda viivitusi.

Soovitus: kontrollida, et tekkida võivad viivitused ei segaks toote kasutamist

[12] https://support.google.com/gemini/answer/13594961?sjid=11958245102865036045-EU#privacy_notice9o5C&zippy=962Cwhat-are-gemini-apps

[13] https://support.google.com/gemini/answer/15229592

[14] https://support.google.com/a/answer/15293691

[15] https://www.google.com/appsstatus/dashboard/

[16] https://workspace.google.com/terms/sla

Kasutusjuhud

Teenuse tulevase võimaliku kasutuse ulatus asutustes võib hõlmata järgmisi andmeid, valdkondi, tegevusi ja vorme:

- isikuandmete töötlemine;
- asutusesiseks kasutamiseks tunnistatud teabe töötlemine;
- memode jm tekstide koostamine, piltide ja videote genereerimine, tekstidest kokkuvõtete koostamine, tekstianalüüs, ideede esilekutsumine, õigusloome, programmeerimiskoodi kirjutamine;
- kasutamine rakendusliidese (AP/) kaudu;

Ametnik suhtleb läbi Gemini kasutajaliidese vestlusrobotiga ja annab sellele korraldusi järgmistel eesmärkidel:

- nõu ja abi saamiseks otsuste tegemisel;
- ideede genereerimiseks;
- reklaam- ja tarbetekstide koostamiseks;
- tekstide toimetamiseks;
- tekstide tõlkimiseks;
- teabe (faktide) ja seletuste küsimiseks;
- etteantud materjalide tõlgendamiseks, neist kokkuvõtete tegemiseks või teabe ülesleidmiseks;
- visuaalide genereerimiseks;
- programmeerimiseks (programmeerimiskoodi koostamiseks ja silumiseks).

Sealjuures võib tekkida vajadus ülaltoodud kasutusviisidega töödelda nii isikuandmeid kui ka asutusesiseseks kasutuseks mõeldud teavet (mis ühtlasi võib sisaldada isikuandmeid).

Sellise kasutusega tekib olukord, kus AI kasutus jääb justkui fakultatiivsena väljapoole ametlikke telgprotsesse.

Kuna tehisaru vestlusrobotid on laialt levinud ka eratarvituses, siis on oluline rõhutada, et kõik käesolevas hinnangus käsitletud asjaolud kohalduvad vaid kasutusele võtva ametiasutuse kontole soetatud litsentsidega teenust kasutades. Eratarbijale mõeldud {tasuta ja tasulised) ekvivalentsed Gemini teenused, mida tarvitsevad kasutada ka ametnikud, alluvad teistsugustele tingimustele. Tähtis on, et ametnikud kasutaksid tööalase teabe töötlemiseks ametiasutuse litsentsiga Gemini kontot, isikliku teabe töötlemiseks aga oma eralitsentsiga seotud kontot.

Gemini featuurid ja teenuse tingimused arenevad kiiresti. Seepärast tuleb kasutuselevõtjal hoida end kursis sellega, mis on kirjas Gemini Apps Privacy Hub-is[17] ja Gemini whitepaperis {ilmub korra aastas)[18].

Soovitus: kontrollida, milliseid andmeid, millise toote versiooniga töödeldakse

EL tehisintellekti määruse kohane riskitase

Gemini teenust vaatleme kui kogust üldotstarbelisi suuri keelemudeleid, mida kasutatakse vestlusroboti teenuse pakkumiseks läbi veebiliidese ja mobiilse seadme rakenduse. Teenuse kasutamine vastavalt kirjeldatud töötlusjuhule klassifitseerub piiratud riskiga tehisintellektiks.

Geminit on võimalik kasutada ka viisidel, mis klassifitseeriksid teenuse suure riskiga või koguni keelatud tehisintellektiks. Selliste kasutusviiside tõkestamiseks on teenustaja juurutanud automatiseeritud meetmeid, kuid ühtlasi on nende vältimine ka ametiasutuse (kasutuselevõtja) pädevuses, seda nii organisatsiooni kui ka

[17] https://support.google.com/gemini/answer/13594961?sjid=11958245102865036045-EU#privacy_notice9o5C&zippy=962Cwhat-are-gemini-apps

[18] https://workspace.google.com/learning/content/gemini-privacy-security-compliance-whitepaper?e=48754805

üksiku ametniku (Gemini kasutaja) tasemel.

Soovitus: luua asutusesisesed protsessid toote kasutamise kontrollimiseks

Rahaline mõju

Gemini teenus on kasutatav osana Google'i kobarteenuse paketist Workspace[19]. Lisaks Geminile kuuluvad kobarasse järgmised pilvteenused:

- Gmail (e-mail),
- Meet (videokonverentsid),
- Drive (pilvtalletus),
- Chat (vestlusside),
- Calendar (ajaplaanimine ja ajakava haldus),
- Docs (tekstiredaktor),
- Sheets (tabelarvutus),
- Slides (slaidiesitlus),
- Vids (videoredaktor),
- Keep (märkmik)
- Tasks (ülesannete haldur)
- AppSheet (rakendusprogrammide ehitaja)
- NotebookLM (tehisarule tuginev allikapõhine teadmuskoostaja).

Workspace'i kobarteenust pakub Google erineva astme pakettides. Astmest sõltub, milline valik ülaltoodud teenusest on kliendile kasutav ning milline on neis teenustes sisalduvate võimete kvaliteet ja maht.

Ühtlasi sisaldavad paketid ka erineval tasemel üldvõimeid Workspace'i kontole (infoturve, tehniline seadistamine ja haldus). Iga kallim pakett sisaldab kõiki soodsamate pakettide teenuseid ja üldvõimeid ning mõnd teenust või üldvõimet lisaks. Kõik paketid sisaldavad Gemini teenust.

Google Workspace'i ametlik hinnakiri[20] ühe kasutaja kohta kuus on järgmine:

- Starter - aastase litsentsiga 6,8C või igakuise litsentsiga 8,IC (sisaldab Gemini vestlusrobotit ja Gemini assistenti GMailis);
- Standard - aastase litsentsiga 13,6C või igakuise litsentsiga 16,2C (sisaldab Gemini vestlusrobotit laiendatud mudeli- ja võimevalikuga ning Gemini assistenti kõikides Workspace'i pilvteenustes, v.a Calendar);
- Plus - aastase litsentsiga 21,IC või igakuise litsentsiga 25,3C (sisaldab Geminit samas ulatuses, mis Standard pakett);
- Enterprise Plus - hind pole avalik, hinnapakkumist tuleb küsida teenustajalt (sisaldab Geminit samas ulatuses, mis Standard pakett).

Soovitus: kontrollida teenuste hindasid vastavalt hinnakirjale

EL/NATO liikmesriigis hoitavad andmed

Teenustaja võimaldab valida regiooni, kus hoitakse Workspace'i, sh Geminis töödeldavaid kliendiandmeid[21]. Regiooni saab vaadata ja muuta Workspace'i kliendi administraator oma menüüsätete kaudu. Regioonivalikus on Ameerika Ühendriigid või Euroopa (tegelikult EL). Ühtlasi on võimalik eraldi määrata nii andmete töötlemise (data in process) kui ka

[19] https://workspace.google.com
[20] https://workspace.google.com/pricing
[21] https://support.google.com/a/answer/15706919?hl=en#zippy=962Cwhere-is-my-organizations-data-processed-and-stored-for-gemini

jõudeandmete (data at rest) talletamise regiooni[22].

Regioonivalikule alluvad andmed on Gemini puhul rakendusele antud käsundid ja sellelt saadud vastused[23].

Google'i andmekeskused asuvad valdavalt Ameerika Ühendriikides ja Euroopas (Soome, Rootsi, Holland, Saksamaa, Poola, Šveits, Itaalia, Hispaania, Belgia, Ühendkuningriik), kuid teenustajal on neid ka kõikides teistes maailmajagudes[24].

Google Workspace'i teenuste andmetaristus on ka suur hulk erinevaid alltöötlejaid paljudest riikidest üle maailma. Alltöötlejad tegelevad teenuste tehnilise korrashoiu, tehnilise toe pakkumise ja turvariskide tuvastamisega[25].

Juhul, kui teenuse pakkumise ja toimepidevuse tagamiseks on teenustajal vajadus edastada kliendi andmeid väljaspool Euroopa Liitu paiknevatele alltöötlejatele, lähtutakse neis toimingutes Euroopa Liidu isikuandmete kolmandatesse riikidesse edastamise standardsetest andmekaitseklauslitest (SCC-s)[26].

GDPR-i kohaselt võib andmeid edastada väljapoole Euroopa Liitu kui on rakendatud asjakohased kaitsemeetmed (artikkel 46[27]).

Andmete asukoht sõltub seega teenuse infrastruktuurist ja Google serverite asukohtadest.

Soovitus: kontrollida, milliseid alltöötlejaid kasutatakse teenuse osutamiseks

Teenusest lahkumise ja andmete ekspordi võimalus

Google'i pilvandmete töötlemise lisa (Cloud Data Processing Addendum[28]) kohaselt võimaldab teenustaja kliendil eksportida oma andmed lepingu kehtivuse vältel. Sama rõhutab teenustaja ka oma kodulehe rubriigis, kus käsitletakse Google'i pilvteenusteid GDPR-i kontekstis[29] (jaotis „Data Retention & Deletion").

Google Workspace'i kliendi administraator saab eksportida kõik kobarteenuses töödeldavad andmed korraga või valikuliselt üksikute kasutajate kaupa. Selle tarbeks on administraatori kasutada andmete eksportimise tööriist (Data Export Tool)[30]. Workspace'i kõrgeima taseme paketis on võimalusi andmeekspordi konfigureerimiseks ja filtreerimiseks veelgi (nt konkreetsete Workspace'i teenuste kaupa, perioodiliselt automatiseeritult jne)[31].

Geminist eksporditakse kasutaja käsundid ja vestlusroboti vastused. Sealjuures on eksportandmestikus igale käsundile kolm vastuseversiooni: vestluses saadud vastus ja kaks vastuse mustandit, mille robot samuti genereeris, ent vestluses ei esitanud[32].

[22] https://support.google.com/a/answer/14310028?hl=en&ref_topic=7631290&sjid=2084291934109486667-EU#zippy=%2Cstep-choose-where-your-data-is-located

[23] https://support.google.com/a/answer/14313033?hl=en

[24] https://cloud.google.com/about/locations/

[25] https://workspace.google.com/intl/en/terms/subprocessors

[26] https://cloud.google.com/terms/data-processing-addendum

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

[28] https://cloud.google.com/terms/data-processing-addendum

[29] https://cloud.google.com/privacy/gdpr

[30] https://support.google.com/a/answer/14339894?hl=en

[31] https://support.google.com/a/answer/1433883#zippy=%2Cexport-features-by-google-workspace-edition

[32] https://support.google.com/a/answer/14817835?sjid=6158129752942721696-EU

Eksportimiseks tellitud andmed ilmuvad allalaadimiseks kliendi Workspace'i pilvtalletuskeskkonda Drive.

Perioodi, kauaks Geminis vestlusi salvestatakse, saab määrata kliendi Workspace'i teenuse administraator. Seadetes on võimalik vestlusajaloo talletamine välja lülitada, sel puhul salvestuvad vestlused kuni 72 tunniks (et teenustaja saaks vajadusel pakkuda nende alusel tuge). Vestlusajaloo lubamise korral on administraatoril võimalik määrata talletusperioodiks kas 3, 18 või 36 kuud[33].

Käsundeid, mis antakse mistahes muus Workspace'i teenuses (nt Gmailis) sinna integreeritud Gemini liidese kaudu, üle sessioonide ei talletata. Need kustuvad peale sessiooni lõppu automaatselt.

Teenuse kasutamise (lepingu) lõppemise järgselt on kliendil võimalik 30 päeva jooksul oma Workspace'i teenustes, sh Geminis töödeldud andmeid jätkuvalt eksportida. Peale seda kustutab teenustaja kõik kliendi andmed 180 päeva jooksul
.
Andmekao vältimiseks peaks andmete omanik hindama Gemini pilvteenuses olevat andmete koosseisu ning nende ajaloolist väärtust, et hinnata, kas andmete eksportimine on vajalik ja otstarbekas.

Soovitus: kontrollida, kas teenusepakkuja kustutab andmed peale lepinguperioodi

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

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid[34].

Teenustajal on järgmised kehtivad sertifikaadid, mille skoobis on Workspace'i kobarteenus ja/või Gemini selle osana:

- ISO/IEC 27017:2015 (kehtib kuni 14.05.2027)
- ISO/IEC 27018:2019 (kehtib kuni 14.05.2027)
- ISO/IEC 27001:2022 (kehtib kuni 14.05.2027)
- ISO/IEC 27701:2019 (kehtib kuni 14.05.2027)
- ISO/IEC 42001:2023 (kehtivuse tähtaega pole avaldatud)
- ISO 9001:2015 (kehtib kuni 10.06.2027).

Workspace'i teenusele, sh Geminile, on tehtud ka auditid:

- SOC 1 Type II
- SOC 2 Type II
- SOC 3[35] [36].

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

[33] https://support.google.com/a/answer/15706919
[34] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[35] https://cloud.google.com/security/compliance/offerings
[36] https://cloud.google.com/security/compliance/compliance-reports-manager#/Region=Global,EMEA&ProductArea=Google_Workspace

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[37].

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)[38]. AI määrus kirjeldab ka, millised on riskitasemed AI süsteemide osas ning reguleerib ka AI süsteemide kasutamist ja 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[39].

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[40].

Soovitus: kontrollida teenusepakkuja vastavust andmekaitsenõuetele

Andmekaitse meetmete rakendamine

Kuna ärikliendid saavad Geminit kasutada vaid Google Workspace'i raames, siis andmekaitset reguleerivad peamiselt just need teenusetingimused (Google Workspace Service Specific Terms)[41]. Gemini kasutamist Google Workspace[42] osana reguleerib andmetöötluslisa (Data Processing Addendum)[43].

Täiesti välistada ei saa ka Google üldiste teenusetingimuste (Terms of Service)[44], Google üldise privaatsuseeskirja (Privacy Policy)[45] ja Gemini Apps privaatsusteatise (Gemini Apps Privacy Notice)[46] kohaldumist mingites olukordades (nt kui siiski kasutatakse kuidagi Gemini Apps lahendust selliselt, et see ei toimu Workspace kaudu).

[37] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[38] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf
[39] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[40] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[41] https://workspace.google.com/terms/service-terms/
[42] https://support.google.com/a/answer/15706919
[43] https://cloud.google.com/terms/data-processing-addendum
[44] https://policies.google.com/terms
[45] https://policies.google.com/privacy
[46] https://support.google.com/gemini/answer/13594961?hl=en#privacy_notice

Sellisel juhul võivad kohalduda teistsugused tingimused, kui on allpool kirjeldatud.

Google Workspace teenusetingimused[47] täpsustavad andmete asukohta ning seda, milliste andmete kohta see käib (mh Geminiga seotud andmete osas).

Generative AI in Google Workspace Privacy Hubis on Google selgitanud, et Google ei jaga kliendisisu (content) kliendi organisatsioonist väljapoole ja kliendisisu ei kasutata tehisintellektimudelite treenimiseks ning seda ei vaata üle inimene. Lisaks täpsustab Generative AI in Google Workspace Privacy Hubis[48] andmete säilitamise tähtaegu, mh viitega andmetöötluslisale.

Andmetöötluslisa[49] kohaselt, kui klient kustutab oma andmeid (Customer Data), siis Google kustutab need andmed oma süsteemidest niipea kui praktiliselt võimalik ning maksimaalselt 180 päeva jooksul, v.a kui seadus nõuab säilitamist. Kui teenuselepingu lõppemisel kohustab Klient Google'it kliendiandmeid (Customer Data) kustutama, siis pärast 30 päevast ooteperioodi kustutab Google andmed niipea kui praktiliselt võimalik ja maksimaalselt 180 päeva jooksul, v.a kui seadus nõuab säilitamist.

Kui klient soovib Google osas läbiviidavat auditit, võib Google auditi eest tasu küsida.

Google kasutab alltöötlejaid https://workspace.google.com/intl/en/terms/subprocessors/. Andmetöötluslisa ja alltöötlejaid arvestades, võib Google andmeid edastada kolmandatesse riikidesse. Google on andmetöötluslisas kirjeldanud, kuidas ta andmeid edastab, kui see vajadus tekib.

Andmetöötluslisa kohaselt teavitab Google klienti ta andmetega seotud intsidendist koheselt ja põhjendamatu viivituseta (promptly and without undue delay), kuid täpsemat aega ei määratleta.

Andmete terviklus on tagatud Google pilvteenuste vastavate meetmetega. Mudelite terviklus tagatakse Responsible Generative AI toolkiti juhendite järgimisega, muuhulgas ollakse läbipaistvad treeningandmete ja nende kvaliteedi osas[50].

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.

Soovitus: kontrollida, millise ajavahemikul teenusepakkuja teavitab intsidendist

Erinõuded

Nõuded teenustajale. Üldotstarbeline tehisintellektimudel peab järgima AI määruse artiklis 50 kirjeldatud läbipaistvuskohustusi.

Tehisaru poolt loodud sisu, näiteks pildid, heli või videofailid, tuleb sellistena selgelt märgistada, et selle sisu edasistel kasutajatel oleks võimalik aru saada, et see on loodud tehisaru abil.

Nõuded kasutusele võtjale. Juhul kui teenusesse sisestatakse isikuandmeid, tuleb järgida isikuandmete kaitse reegleid, mh hinnata andmekaitse mõjuhinnangu vajalikkust ja vajadusel see läbi viia. Samuti tuleb arvestada muude kohalduvate õigusaktidega (näiteks avaliku teabe seadus).

[47] https://workspace.google.com/terms/service-terms/
[48] https://support.google.com/a/answer/15706919
[49] https://cloud.google.com/terms/data-processing-addendum
[50] https://workspace.google.com/learning/content/gemini-privacy-security-compliance-whitepaper?e=48754805

Gemini teenuse kasutamisel tuleb järgida teenuse kasutamise reegleid (Generative AI Prohibited Use Policy)[51]. Teenust ei tohi kasutada järgmisteks tegevustes ega eesmärkidel:

- laste seksuaalseks väärkohtlemiseks või ärakasutamiseks;
- vägivalla või terrorismi õhutamiseks;
- enesevigastamisele õhutamiseks;
- teisi isikuid imiteerivate intiimsete kujutiste loomiseks ilma asjaomaste isikute nõusolekuta;
- muu ebaseaduslikku tegevuse hõlbustamiseks, näiteks juhiste saamiseks ebaseaduslike ainete, kaupade või teenuste valmistamiseks või neile juurdepääsuks;
- privaatsuse ja intellektuaalse omandi õiguste rikkumiseks, näiteks isikuandmete või biomeetria kasutamiseks seaduses nõutava nõusolekuta;
- teiste inimeste jälgimiseks või kontrollimiseks ilma nende nõusolekuta;
- automatiseeritud otsuste tegemiseks ilma inimjärelevalveta kõrge riskiga valdkondades, näiteks tööhõive, tervishoiu, rahanduse, õigus-, eluaseme-, kindlustus- või sotsiaalhoolekande valdkonnas;
- rämpspostituste ja õngitsuste tegemiseks või pahavara loomiseks ja levitamiseks;
- Google'i või muu taristu või teenuste kuritarvitamiseks, kahjustamiseks, või häirimiseks;
- kuritarvituskaitse meetmetest või turvafiltritest möödahiilimiseks, näiteks mudeli manipuleerimiseks selliselt, et see oleks siintoodud eeskirjadega vastuolus;
- vihakõne loomiseks ja levitamiseks;
- vägivallale õhutamiseks;
- teiste isikute ahistamiseks, kiusamiseks, hirmutamiseks, väärkohtlemiseks või solvamiseks;
- seksuaalse sisu loomiseks, näiteks pornograafia;
- valeinformatsiooni ja eksitava teabe loomiseks ja levitamiseks;
- pettuste ja kelmuste tegemiseks;
- isiku {elusa või surnud) jäljendamisega ilma, et oleks selgesõnaliselt avaldatud, et tegu on loodud jäljendusega;
- väärekstpertsuse loomiseks ja levitamiseks tundlikes valdkondades - näiteks tervishoius, rahanduses, valitsusteenustes või õiguses;
- eksitavate väidete levitamiseks valitsus- või demokraatlike protsesside kohta või kahjulike tervisepraktikate kohta;
- genereeritud sisu masinloomelise päritolu moonutamiseks või varjamiseks.

Soovitus: kontrollida, et teenust ei kasutataks keelatud viisil

Turvameetmete rakendamine

Gemini Appsi käitatakse Google'i pilvetaristul, mis on projekteeritud turvalisena[52] ning rakendatud on Google'i andmekeskuste ja võrguliikluse turvameetmed[53].

Google lubab, et on Workspace'i kliendiandmete kaitseks rakendanud

[51] https://policies.google.com/terms/generative-ai/use-policy

[52] https://cloud.google.com/security/infrastructure?hl=en

[53] https://cloud.google.com/docs/security/overview/whitepaper

tehnilisi, korralduslikke ja füüsilisi meetmeid (safeguards)[54].

Nii jõude kui liikvel andmed on krüpteeritud vastavate Google'i pilve krüpteerimismehhanismidega[55] [56].

Turvaliseks sisselogimiseks on võimalik kasutada pääsuvõtit (passkey) või turvavõtit (security key), mitmikautentimist või topeltkontrolli (two-step verification)[57]. Kasutajat teavitatakse ebatavalistest tegevustest tema kontol, samuti annab Google talle turvalisusealaseid soovitusi (security checkup).

Kasutaja Geminiga töödeldavate failide hoiukoht on Google Drive, neile kehtivad Workspace'is seatud õigused (ka Gemini jaoks)[58].

Workspace'i administraator saab reeglitega (Trust rules Google Drive'is) piirata failide jagamist, assistendi kaudu tehtavat andmevargust (data exfiltration) jms. Faile, mille printimine, allalaadimine või kopeerimine on kasutajale keelatud, ei kasuta ka Gemini oma vastuse koostamisel.

Administraatoril on võimalik saada ülevaade andmetele seatud juurdepääsupiirangutest ja kuidas neid on kasutatud (Drive inventory reporting), samuti näha, kes kui palju Geminit kasutab. Logisid failide kasutamise kohta Gemini poolt saab eksportida vastava APIga Google Drive'i.

Gemini kasutamist erinevates Workspace'i rakendustes saab administraator sisse või välja lülitada, samuti keelata või lubada konkreetsel kasutajal mõnd Gemini äppi kasutada. Defineerides juurdepääsutasemed (access levels) saab juurdepääsu reguleerida lähtudes kasutajast, tema seadmest, IP aadressist või asukohast[59]. Sätteid, mida turvalisuse ja andmetele juurdepääsu osas kliendi administraatoril on võimalik seadistada, on kirjeldatud[60].

Prompti ohutust hindab Gemini enne käivitamist ja vajaduse korral teavitab kasutajat ohust[61].

Frontline Plus; Enterprise Plus; Education Standard and Education Plus puhul on toetatud krüpteerimine kliendi juures (client-side encryption (CSE)),[62] see võimaldab piirata Gemini juurdepääsu tundlikele andmetele; ühelgi Google süsteemil ega töötajal pole sisule sel juhul juurdepääsu.

Osad litsentsid sisaldavad tööriista Security investigation tool[63].

On näidatud edukaid promptisiüsti (prompt injection) ründeid, kus e-kirjasse peidetud tekstiga manipuleeriti assistent väljastama eksitavat väljundit, nt Gmaili kokkuvõtet[64].

Ettevõte tunnistab ründevektori olemasolu ja soovitab administraatoritel suhtuda Gmaili kokkuvõtetesse ettevaatusega ning rakendada õngitsustevastaseid meetmeid.

Google deklareerib, et teenuse kasutamise reeglite järgimise tagamiseks on juurutatud meetmeid, mis aitavad teenuse väärtarvitusi tuvastada ja tõkestada. Meetmed hõlmavad nii automatiseeritud

[54] https://workspace.google.com/terms/premier_terms/
[55] https://cloud.google.com/docs/security/encryption/default-encryption
[56] https://services.google.com/fh/files/misc/gws_security_whitepaper.pdf
[57] https://landing.google.com/advancedprotect
[58] https://workspace.google.com/security/ai-privacy/
[59] https://support.google.com/a/answer/9261439?hl=en&sjid=l6230191034105272886-NA
[60] https://support.google.com/a/topic/7556782?hl=en&ref_topic=l0012113&sjid=l205108941007511959-EU
[61] https://workspace.google.com/blog/ai-and-machine-learning/enterprise-security-controls-google-workspace-gemini
[62] https://support.google.com/a/answer/10741897
[63] https://support.google.com/a/answer/7575955?hl=en&sjid=l6040906469908561115-NC
[64] https://www.tomsguide.com/computing/online-security/google-gemini-for-workspace-has-been-exploited-to-send-emails-with-hidden-malicious-messages

protsesse kui ka inimeste tehtavaid ülevaatusi[65].

Iga Geminis tehtud päringut ja vastust kontrollitakse põhjaliku ohutusatribuutide loendi vastu, et tõkestada sisu, mis rikub teenuse kasutamise reegleid[66].

Sealjuures on juurutatud meetodid, mis aitavad tõkestada pahatahtlikke käsundeid (prompt injection), pahatahtlikke linke ja ohutusfiltritest mööda hiilimise katseid (Gemini for Google Workspace privacy, security, and compliance white paper, lk 10).[67]

Kui Google on tuvastanud eeskirja rikkumise, saab kasutaja sellest teate kas Gemini kasutajaliideses või e-postiga. Korduvate rikkumiste korral ja rikkumiste tõsidusest sõltuvalt võib Google piirata juurdepääsu Gemini teenusele või Google'i kontole. Pole selge, kas juurdepääsu võidakse piirata ainult tingimusi rikkunud lõppkasutajale või ka kogu kliendikonto {asutuse) tasemel.

Soovitus: rakendada asutusesiseseid infoturbe meetmeid toote turvaliseks kasutamiseks

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.**
Intellektuaalse omandi osas rikkumine, kui pole selge, kellele vastutus kuulub. Kiired regulatiivsed muudatused võivad kaasa tuua keelde AI kasutuselevõtu osas või liigselt

[65] https://support.google.com/gemini/answer/16625148

[66] https://docs.cloud.google.com/gemini/docs/discover/responsible-ai

[67] https://workspace.google.com/learning/content/gemini-privacy-security-compliance-whitepaper?e=48754805

AI-ga seotud riskid	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

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

Gemini pakub klientidele rohkeid võimalusi, kuidas muuta kasutajate töö produktiivsemaks ja kulutõhusamaks. Google klientidel on võimalus seadistada Gemini pilvteenuse 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 Gemini teenuse katkematust tööst.

Vajalik on rakendada täiendavaid meetmeid paralleelselt Gemini kasutamisega, mh koolitada kasutajaid, arendada alternatiivseid töömeetodeid, kontrollida Google kätte saadavaid andmeid jms.

Arvestada tuleks, et AI kasutamise reguleerimine EU tasandil on alles algusfaasis ning puuduvad ka regulatsioonid kohalikul tasandil, mis annaksid selgeid suuniseid AI kasutamiseks.

Asutus peab hindama, milliste kasutusjuhtude korral on Gemini sobiv kasutamiseks. Arvesse tuleks võtta AI kasutamisega ja pilvtoodetega seonduvaid riske ning Google poolt rakendatud meetmeid turvalisuse tagamiseks.