Perplexity

Kirjeldus

Käesolev usaldusväärsuse hinnang keskendub Perplexity AI, Inc. pilvtöötlusteenuse (edaspidi Perplexity) riskide kirjeldamisele ning ei kohaldu 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[1].

Perplexity on otsingmootor, mis kasutab tehisintellekti veebiotsinguteks ning vastuste tagastamiseks koos allikatega. SaaS - Perplexity on tehisintellektiga otsingumootor - küsimuse järel otsib teenus veebist vastavat teemat ning tagastab vastused koos allikatega.[2]

Perplexity asutati 2022. aastal Aravind Srinivas, Denis Yarats ja Andy Konwinski poolt. 2023. aasta märtsis avaldas firma, et neil on kaks miljonit aktiivset kasutajat ning 2024. aasta alguseks oli neil kümme miljonit aktiivset kasutajat.[3]

Perplexity on kaheksa rahastusvooruga kaasanud kokku 1,02 miljardit dollarit. Suurim rahastusring oli 500 miljoni dollari suurune C-seeria 2024. aasta detsembris.[4]

Kasutajate seas on tarkvara hinnatud tööriistana, mis on lihtsasti kasutatav, töötab kiiresti ning tagastab täpsed vastused koos usaldusväärsete allikaviidetega. G2 keskkonnas on seda hinnatud keskmise hindega 4,7 5-st.[5]

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

Teenuse võimalused

Otsingu tegemiseks on võimalik kasutada erinevaid mudeleid[6]:

- Sonar (Perplexity enda mudel; põhineb Meta LlaMa 3.1 708 avakoodmudelil, aga on edasi treenitud Perplexity poolt)
- GPT
- DALL-E

[1] Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[2] https://www.perplexity.ai/help-center/en/articles/10352155-what-is-perplexity
[3] https://golden.com/wiki/Perplexity-X9D5GWB
[4] https://tracxn.com/d/companies/perplexity/V2BE-SihMWJlhNb2_ulW7Gry25JzPFCBg-iNWi94XI8/funding-and-investors#funding-rounds
[5] https://www.g2.com/products/perplexity/reviews
[6] https://www.perplexity.ai/hub/legal/third-party-models

- o mudelid
- Claude mudelid
- Grok mudelid
- Gemini mudelid
- Vea mudelid
- FLUX.1

Otsinguid on võimalik teha erineval tasemel. Esiteks on concise searches ehk pinnapealsed otsingud igapaevasteks küsimusteks. Järgmine kategooria on pro queries, mille puhul kasutatakse mitmejärgulist arutlemist ning tagastatakse rohkem allikaid. Samuti on võimalik teha süvauuringut (deep research queries), mis tagastab põhjaliku raporti. Teenust on võimalik kasutada brauseris, töölauarakendusena, iPhone äpina ja Android äpina.[7]

Otsingut tehes on võimalik täpsustada, millistest allikatest infot otsida. Vaikeseadena saab otsida infot kogu veebist. Lisaks sellele saab infot otsida teadustöödest ja enda poolt üles laetud failidest.

Teenus kogub andmeid, et parandada ja personaliseerida kogemust. Kui klient on loonud konto, siis kogutakse tema personaalseid andmeid, aga neid ei müüda kolmandatele osapooltele.[8]

Samuti pakutakse teenust nimega Perplexity Lab. Kui tavaline Perplexity otsingumootor vastab kasutaja konkreetsele küsimusele põhjaliku analüüsiga, siis Perplexity Lab läheb sammu kaugemale ning loob tervikliku projekti mitmete komponentidega. Labs on võimeline genereerima faile, slaidiesitlusi, pilte, miniäppe ja muid interaktiivseid elemente.[9]

Lisaks sellele pakub Perplexity teenust nimega Comet - tehisintellektiga brauser. Selle eesmärk on olla kasutaja personaalne assistent ja mõttepartner, mis aitab suurendada keskendumist ja muuta töö tegemise sujuvaks. Comet võimaldab vastata meilidele, plaanida koosolekuid, teha põhjalikku otsingut ja sooritada Internetis oste.[10]

Perplexity on lehekülg, kus on näha kõigi nende teenuste staatused[11]. Sealt ilmneb, et 2025. aasta esimeses kvartalis oli veebilehe aktiivaeg 99,93% ja API aktiivaeg 100,0%. Teise kvartali puhul on need numbrid vastavalt 99,94% ja 100,0% ning kolmanda kvartali puhul 100,0% ja 100,0% (02.09.2025 seisuga.

EL tehisintellekti määruse kohane riskitase

Perplexity teenust vaatleme kui hulka üldotstarbelisi suuri keelemudeleid, mida kasutatakse juturoboti teenuse pakkumiseks läbi veebiliidese. Teenuse kasutamine vastavalt kirjeldatud töötlusjuhule klassifitseerub minimaalse riskiga tehisintellektiks.

Perplexity teenust on võimalik kasutada ka viisidel, mis klassifitseeruvad suure riskiga tehisintellektiks või keelatud tehisintellektiks. Kasutusreeglid võivad sellist kasutust piirata.

Soovitus: kontrollida, et teenust ei kasutataks keelatud viisil

[7] https://www.perplexity.ai/help-center/en/articles/10352155-what-is-perplexity
[8] https://www.perplexity.ai/help-center/en/articles/10354855-what-data-does-perplexity-collect-about-me
[9] https://www.perplexity.ai/help-center/en/articles/11144811-perplexity-labs
[10] https://www.perplexity.ai/comet
[11] https://status.perplexity.com/

Kasutusjuhud

Standardloetelu viisidest, kuidas teenust saab kasutada:

- infootsing;
- põhjaliku ülevaate saamine konkreetsest teemast;
- analüüside tegemine;
- allikate ja viidete leidmine;
- piltide genereerimine;
- slaidiesitluste genereerimine.

Artiklis[12] antakse soovitusi Perplexity klientidele: a) dokumenteerida kõik tegevused teenuses; b) hinnata promptidega, jälgimisega ning andmeedastusega seotud riske; c) nõuda tõendusi andmete asukoha, kustutamise ajavahemike ja krüpteerimise osas; d) Androidi äppi kasutada üksnes konteineris; e) kasutada vaid turvaliste brauserite, VPN ja rollipõhise pääsukontrolliga; f) vältida isikuinfo ja konfidentsiaalsete andmete sisestamist; g) luua selged reeglid tundlikel aladel (nagu HR, õigusvaldkond ja finantsala) kasutamiseks; h) lasta Perplexity teenusest saadud tulemused enne taaskasutust juristil üle vaadata. Tõenäoliselt kehtivad need juhised ka teiste AI-teenuste puhul.

Rahaline mõju

Pakett Perplexity Free on tasuta pakett, mis võimaldab piiratud koguses otsinguid. Tavaotsingud on piiramatud, 3 pro queries päeva kohta, 3 deep research queries päeva kohta ja maksimaalselt 5 üleslaaditud faili.

Pakett Perplexity Pro maksab 20 dollarit kuus. Selle paketiga on tavaotsingud piiramatud, pro queries piiramatud, 500 deep research queries päeva kohta ja maksimaalselt 50 faili üleslaadimine. Samuti lisandub võimalus valida, millise mudeliga otsingut tehakse ning juurdepääs Perplexity Labs osale.

Pakett Perplexity Enterprise Pro maksab 40 dollarit kuus või 400 dollarit aastas. Selle paketi piirangud on üldiselt samad nagu Perplexity Pro paketi puhul. Lisandub võimalus turvalisusega seotud seadistusteks (nt kasutajate haldus).

Pakett Perplexity Max maksab 200 dollarit kuus või 2000 dollarit aastas. See pakett sisaldab kõike, mis on Pro paketis. Lisaks sellele saab kasutaja piiramatu ja kiirema ligipääsu uutele mudelitele ja funktsionaalsustele. Samuti saavad Max kasutajad juurdepääsu Comet brauserile.

Pakett Perplexity Enterprise Max maksab 325 dollarit kuus või 3250 dollarit aastas. See pakett sisaldab kõike, mis on Enterprise Pro paketis. Lisaks sellele saab näiteks teha piiramatu koguse päringuid, genereerida 15 kõrge kvaliteediga videot

[12] https://heydata.eu/en/magazine/perplexity-ai-and-data-protection-how-secure-is-your-data-really

kuus ja ligipääsu kõrgema taseme mudelitele.[13][14].

Soovitus: kontrollida hinnakirja ning kaasnevaid kulusid

EL/NATO liikmesriigis hoitavad andmed

Perplexity kasutab mitmeid kolmandaid osapooli, kes tegelevad erinevate andmetega (k.a isikuandmetega). Nendeks kolmandateks osapoolteks on AWS, Microsoft Azure, Anthropic, Google, Amazon Bedrock, xAI, Loops.so, OpenAI, Orb ja Stripe. Kõik need osapooled hoiavad andmeid Ameerika Ühendriikides.[15]

GDPR-i kohaselt võib andmeid edastada väljapoole Euroopa Liitu kui on rakendatud asjakohased kaitsemeetmed (artikkel 46[16]).

Soovitus: kontrollida, kus andmeid majutatakse

Teenusest lahkumise ja andmete ekspordi võimalus

Kasutajal on võimalik oma vestluste sisu alla laadida. Võimalikud ekspordivormingud on PDF, Markdown ja DOCX. Avalikud materjalid ei maini, et oleks võimalik alla laetud vestluste uuesti üles laadimine või vestluste taastamine.
Kasutaja vestlusi hoitakse alles tähtajatult. Kui vestlus on kustutatud, siis seda ei saa enam taastada. Kogemata vestluste kustutamise vältimiseks kasutatakse kinnitusküsimusi.[17]

Varunduse kohta väidab Perplexity vaid, et see on olemas ja kirjeldab nõuded kliendiandmete varundamiseks ja taasteks.[18]

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

Soovitus: kontrollida üle, millised on võimalused andmete varunduseks

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

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid[19].

Firma on läbinud auditi aruande SOC 2 Type 2 tegemise American Institute of Certified Public Accountants (AICPA) poolt. Nad väidavad, et on kooskõlas GDPR ja HIPAA reeglitega ning vastavad PCI nõuetele.[20] Nad on ka osa DPF (Data Privacy Framework) programmist[21].

AI juurutamisel tuleks lähtuda juhtimissüsteemi rakendamisest, nt

[13] https://www.perplexity.ai/enterprise/pricing
[14] https://www.perplexity.ai/help-center/en/articles/11680686-perplexity-max
[15] https://trust.perplexity.ai/subprocessors
[16] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&qid=1689851996164
[17] https://www.perplexity.ai/help-center/en/articles/10354769-what-is-a-thread
[18] https://trust.perplexity.ai/controls
[19] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[20] https://www.perplexity.ai/enterprise/security
[21] https://www.dataprivacyframework.gov/list

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[22].

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)[23]. 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

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

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

komponenti (sh selle riskitase) süsteemis kasutatakse [24].

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[25]. Täpsemalt on kirjeldatud Microsofti usaldusväärsuse hinnangus.

Soovitus: kontrollida üle andmekaitse nõuetele vastavus

Andmekaitse meetmete rakendamine

Andmetöötlust Perplexity ärikasutajate (enterpise customer) puhul reguleerivad peamiselt ärikliendi teenuseleping (Perplexity Enterprise Pro Terms and Conditions)[26] ja andmetöötluslisa (Data Processing Addendum)[27]. Arvestada tuleb, et muude teenuste või muul kujul (nt API) teenuste kasutamisel võivad kohalduda muud oluliselt erinevad (nt konfidentsiaalsuse osas) tingimused.

Teenuselepingu kohaselt ei või Perplexity kasutada kliendisisu (Customer Content), tehisintellektimudelite[28] treenimiseks, üle treenimiseks ega täiustamiseks). Andmetöötluslisa täpsustab, et Perplexity ei tohi isikuandmeid kasutada keelemudelite treenimiseks[29].

Perplexity kasutab kolmandate isikute suuri keelemudeleid ning klient peab arvestama nende keelemudelite tingimuste ja lepingutega. Teenuseleping sisaldab üldist konfidentsiaalsusklauslit[30].

Andmetöötluslisa kohaselt kinnitab klient, et temapoolne isikuandmete töötlemine on kooskõlas kõikide kohalduvate isikuandmete kaitse õigusaktidega ja tal on kõik vajalikud õigused, load ja nõusolekud, et isikuandmeid Perplexity-le avaldada, võimaldades neid Perplexityl töödelda.

Andmetöötluslisa keelab Perplexity-l isikuandmeid müüa või jagada, säilitada muul eesmärgil kui Perplexity ja kliendi vahelisest teenuselepingus kokku lepitud ärisuhe ning kombineerida muude või mujalt saadud isikuandmetega.

Isikuandmetega seotud rikkumise korral peab Perplexity klienti teavitama ilma põhjendamatu viivituseta alates hetkest, mil Perplexity sai rikkumisest teada. Täpsemat aega ei ole sätestatud.

Kui Perplexity lõpetab kliendile teenuste osutamise, peab Perplexity 30 päeva jooksul kustutama või tagastama (kliendi valikul) kõik isikuandmed, v.a. kui säilitamist nõuavad õigusaktid.

Perplexity võib töödelda isikuandmeid kolmandates riikides ning on seda andmetöötluslisas kirjeldanud.

Perplexity kasutab alltöötlejaid. Nimekiri alltöötlejatest on leitav andmetöötluslisa[31] lisast 2 (Annex 2).

Lubatud kasutuspoliitika (Acceptable Use Policy)[32] kohaselt peab kasutaja:

- järgima kehtivaid seadusi;
- vältima kõrge riskiga tegevusi;

[24] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[25] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[26] https://www.perplexity.ai/hub/legal/enterprise-terms-of-services
[27] https://www.perplexity.ai/hub/legal/dpa
[28] https://www.perplexity.ai/hub/legal/enterprise-terms-of-services
[29] https://www.perplexity.ai/hub/legal/dpa
[30] https://www.perplexity.ai/hub/legal/enterprise-terms-of-services
[31] https://www.perplexity.ai/hub/legal/dpa
[32] https://www.perplexity.ai/hub/legal/aup

- vältima tehnilist vaarkasutust;
- järgima kolmandate osapoolte kasutuspoliitikaid.

Perplexity on seadnud mitmed reeglid selle kohta, mida kasutaja ei tohi teenuse kasutamisel teha ([33], peatükk 5.2).

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, millised on kaasatud alltöötlejad

Turvameetmete rakendamine

Organisatsioonid, kellel on ranged nõuded, et Perplexity süsteemide ja kliendiandmete kaitseks rakendatud turvameetmete kirjelduste allikad on[34][35].

Ettevõtte töötajate juurdepääsu tootmiskeskkonnale haldab AWS 1AM. Kasutatakse ainulogimist {SSO), mitmikautentimist {MFA), pääsumandaatide piiratud kehtivusaega; tundlike ressursside puhul lisaks ajutisi juurdepääsumeetmeid (Just-In- Time (JIT) access controls). Juurdepääsud vaadatakse üle vähemalt kord kvartalis. Rangelt on keelatud talletada kliendiandmeid tööarvutites või irdkandjatel.

Tootmiskeskkonna eraldamiseks teistest keskkondadest on see loodud omaette AWS konto, juurdepääsude ja võrguseadistustega. Kasutatakse Wizi {pilvekeskkondade seire) ja Cloudflare' teenuseid {teenustõkestusrünnete kaitse, Web Application Firewall {WAF), sidekanali krüpteerimist {SSL/TLS)). Otspunktidel on tugevad paroolid, kettakrüpto, kaugkustutamise võimekus, EDR-tehnoloogia jms.

Panther SIEMi abil analüüsitakse kriitiliste ressursside logisid, et tuvastada turvarikkemärke (indicator of compromise, /OC), käitumismustrite anomaaliaid ja kõrvalekaldeid poliitikatest.

Turvameeskond on kättesaadav ööpäevaringselt.

Lisaks iga-aastasele välise partneri läbistustestimisele on olemas vigade avalikustamise programm (Vulnerability Disclosure Program, VOP)[36] ja veaotsingu tasuprogramm (bug bounty program).

Igal aastal viiakse läbi alltöötlejate ja tarnijate riskihindamine; tarnijate puhul on vaatluse all on töödeldavate andmete tundlikkus, Perplexity sõltuvus tarnijast ning tarnija maine.

Kestlikkuse tagamiseks on võetud küberkindlustus.

Enterprise Pro klientidel on võimalik seadistada SSO ning saada reaalajas teavitusi kahtlase või riskantse käitumise kohta[37][38]. Kliendi administraator saab Security Hubis keelata või lubada failide jagamist ning üles- ja allalaadimist, connectoritega ühendumist, defineerida kasutatavate LLM-ide valikut jm[39].

Enterprise Max pakub lisaks Pro paketis sisalduvale: otspunktkrüpteerimist, paindlikumaid juurdepääsude seadmise

[33]https://www.perplexity.ai/hub/legal/terms-of-service
[34]https://www.perplexity.ai/enterprise/security
[35]https://trust.perplexity.ai/
[36]https://www.perplexity.ai/hub/security-vdp
[37]https://www.perplexity.ai/help-center/en/articles/10352973-what-is-enterprise-pro
[38]https://www.perplexity.ai/hub/blog/how-perplexity-enterprise-pro-keeps-your-data-secure
[39]https://www.perplexity.ai/help-center/en/articles/ 12053065-enterprise-organization-permissions

viise kasutajatele, revisjonilogi (audit logs) ja seadistatavat andmesäilituspoliitikat[40].

Augustis 2025 avaldatud analüüsis[41] juhib tähelepanu sellele, et Perplexity turvaline kasutamine on suuresti kasutaja vastutus. Näiteks

•ei ole privaatsuse tagamine teenusesse sisse ehitatud (privacy by design), vaid isikuandmete kasutamine mudelite treenimiseks tuleb eraldi valja lülitada (opt out);

•kasutajate tegevusi ja käitumist jälgitakse jälitusküpsiste (tracking cookies abil ning analüüsitakse kolmanda osapoole {nt Google Analytics) abil;

•Perplexity Androidi äpil on tuvastatud nõrkusi; kui seda kasutada, siis konteineris;

•ettevõte ei ole avalikustanud turvaauditite tulemusi;

•Al - ohutusmeetmete osas tuginetakse kolmandate osapoolte lahendustele, Perplexity ise ei tee omalt poolt nt semantilist filtreerimist (semantic filtering) vm.

Soovitus: kontrollida teenusepakkuja poolt tagatud turvameetmete rakendamist

Erinõuded

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

Tehisaru poolt loodud sisu, näiteks pildid, heli või videofailid, tuleb sellistena selgelt märgistada, et sellise sisu edasistel kasutajatel oleks võimalik tuvastada, 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).

Enne kolmandate osapoolte mudelite integreerimist hindab Perplexity nende ohutusmeetmeid ja sobivust Perplexity eesmärgiga pakkuda täpset, kasulikku ja vastutustundlikku otsingukogemust[42].

Allikas[43] mainib Enterprise Pro paketi ohutusmeetmete seas „robustseid" kaitsepiirdeid, ent enamat nende kohta ei täpsustata.

Augustis 2025 väideti, et Perplexity tugineb Al-ohutusmeetmete osas ainult kolmandate osapoolte lahendustele, ise mingisuguseidki Al-spetsiifilisi meetmeid rakendamata[44]. Oktoobris teadvustati Perplexity's promptisi.isti (prompt injection) võimalus ning avaldati Cometi kaitse kohta on eraldi ülevaade[45]. Muid teenustajapoolseid Al-ohutusmeetmete kirjeldusi avalikest allikatest ei tuvastatud.

Soovitus: kontrollida, kas teenus vastab Al määruses väljatoodud nõuetele

[40] https://www.perplexity.ai/help-center/en/articles/12310544-what-is-enterprise-max

[41] https://heydata.eu/en/magazine/perplexity-ai-and-data-protection-how-secure-is-your-data-really

[42] https://www.perplexity.ai/hub/legal/third-party-models

[43] https://www.perplexity.ai/hub/ blog/how-perplexity-enterprise- pro-keeps-your-data-secure

[44] ttps://heydata.eu/en/magazine/perplexity-ai-and-data-protection-how-secure-is-your-data-really

[45] https://www.perplexity.ai/hub/blog/mitigating-prompt-injection-in-comet

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 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.**

AI-ga seotud riskid	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

Perplexity on rakendanud infoturbe ja andmekaitse alaseid meetmeid, millega saab lugeda Perpelexity teenus usaldusväärseks. Perpelxity andmete majutamise asukohta pole võimalik tuvastada, mistõttu ei saa kinnitada, kas andmekaitse nõuded on täidetud.

Perplexity pakub klientidele rohkeid võimalusi, kuidas muuta kasutajate töö produktiivsemaks ja kulutõhusamaks. 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 Perplexity teenuse katkematust tööst.

Vajalik on rakendada täiendavaid meetmeid paralleelselt Perplexity kasutamisega, mh koolitada kasutajaid, alternatiivsete töömeetodite arendamine, Perplexityle kätte saadavate andmete kontrollimine 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 Perplexity sobiv kasutamiseks. Arvesse tuleks võtta AI kasutamisega ja pilvtoodetega seonduvaid riske ning Perplexity poolt rakendatud meetmeid turvalisuse tagamiseks.