Notion

Kirjeldus

Käesolev usaldusväärsuse hinnang keskendub Notion Labs, Inc. pilvtöötlusteenuse (edaspidi Notion) riskide kirjeldamisele ning ei kohaldu Notion Labs, Inc. 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].

Notion on tootlikkuse ja plaanimise töövahend, mis võimaldab teha märkmeid ja korraldada ülesandeid. Isiklikuks kasutamiseks on see tasuta, kuid tasu eest lisanduvad täiendavad funktsionaalsused, näiteks tiimides kasutamine, integratsioon teiste teenustega (näiteks Slack, Google Drive, GitHub) ja teatud funktsionaalsuste piiramatu kasutamine.

Notion on asutatud 2016. aastal Ameerika Ühendriikides ning selle asutajad on Chris Prucha, Ivan Zhao, Jessica Lam, Simon Last ja Toby Schachman[2]. Peakontor asub San Franciscos, aga firmal on kontorid ka linnades New York, Dublin, Hyderabad, Tokyo, Seoul ja Sydney[3].

Nad teevad koostööd organisatsiooniga ROOST (Robust Open Online Safety Tools), mille eesmärk on luua turvalisemaid süsteeme AI ajastul.[4]

Kasutajate seas on tarkvara hinnatud kui tööriist, kuhu on koondatud kõik võimalused ning mis on lihtsasti kohandatav, G2 keskkonnas on seda hinnatud keskmise hindele 4,7 5 - st[5].

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

Toote võimalused

SaaS - Notion on töö tootlikkuse, plaanimise ja korraldamise töövahend, mille eesmärgiks on hallata kõike ühest kohast. See võimaldab teha märkmeid, märkida kalendrisündmusi, korraldada ülesandeid ja hallata andmebaasi. Lisaks on võimalik Notionisse integreerida ka teisi teenuseid, nt Google Drive, Google Gmail, Slack, Github, Gitlab ja Asana.

Notion on vaga paindlik keskkond, mis võimaldab täidetavate sisulehtede ülesehitust just sellisel viisil, mis on kasutaja jaoks loogiline ja kasutamiseks mugav. Avaleheks on tühi valge leht, kuhu

[1]

[2] https://system.privco.com/company/notion-labs

[3] https://www.notion.com/careers

[4] https://www.notion.com/help/ai-safety

[5] https://www.g2.com/se11ers/notion-7effc4fe-47b3-4888-8ef0-ce4addda94db

kasutaja saab lisada endale meelepäraseid komponente. Teksti saab vormindada täpploendiks, koodilõiguks, tabeliteks ja graafikuteks. Samuti saab lisada pilte, videoid, linke, faile ja palju muud. Iga komponenti on võimalik tõsta ja paigutada ümber. Igale lehele saab lisada alamlehti, mis omakorda tekitab puustruktuurist failisüsteemi.

Notionit on võimalik kasutada brauseris, töölauarakendusena ja mobiilirakendusena. Funktsionaalsus nimega Notion AI[6] on saadaval Business and Enterprise pakettides. Seda saab kasutada tekstist kokkuvõtte tegemiseks, ajurünnaku läbiviimiseks või diagrammide genereerimiseks. Notion AI kasutab mudeleid GPT - 4, Anthropic Claude, Deepl ja Fireworks[7][8]. Vestlusrobot (Personal Agent) kasutab kontekstina kõiki materjale kasutaja tööalast (workspace) ja ühendatud teenustest (connected apps), nt Google Drive'ist voi Slackist.

Garanteeritud aktiivaeg (uptime) on 99,9%[9]. Erinevate teenuste seisu on võimalik jälgida kodulehel[10] ning see leht sisaldab infot ka varem toimunud sündmuste kohta.

Taaste sihtkestvuseks (RTO, recovery time objective) on eeldatud kaks tundi, taaste sihtseisuks (RPO, recovery point objective) 24 tundi[11].

Kasutusjuhud

Standardloetelu viisidest, kuidas teenust saab kasutada:

- projektide haldamine;
- tööülesannete haldamine;
- igapäevatöö plaanimine;
- koosolekute ja kohtumiste planeerimine;
- koosoleku märkmete tegemine;
- märkmetest kokkuvõtte tegemine (tehisintellektiga);
- ajurünnakud (tehisintellektiga);
- teabe (faktide) ja seletuste küsimine.

EL tehisintellekti määruse kohane riskitase

Teenuse kasutamine vastavalt kirjeldatud töötlusjuhtudele liigitub minimaalse riskiga tehisintellektiks.

Notioni teenust on võimalik kasutada ka viisidel, mis liigituksid suure riskiga tehisintellektiks või keelatud tehisintellektiks. Eriti suureks ohuks on väliste teenuste integreerimine ning selle kaudu tundlikele andmetele ligi pääsemine.

Soovitus: kontrollida, milliste teenustega on võimalik toodet integreerida

Rahaline mõju

Isiklikuks kasutamiseks on tööriist tasuta {pakett nimega Free), sellega on võimalik teha märkmeid, hallata andmebaase, plaanida tegevusi, kasutada Notioni kalendrit.

Järgmise taseme pakett on nimega Plus, mõeldud väikestele tiimidele ning maksab 9,50 eurot kuus ühe liikme kohta (aastakaupa makstes; kuukaupa makstes on ühe kuu tasu 11,50 eurot). Selle paketiga

[6] https://www.notion.com/help/notion-ai-faqs
[7] https://www.notion.so/notion/Notion-s-List-of-Subprocessors-268fa5bcfa0f46b6bc29436b21676734
[8] https://www.notion.com/help/guides/everything-you-can-do-with-notion-ai
[9] https://www.notion.com/security
[10] https://www.notion-status.com
[11] https://www.notion.com/help/security-and-privacy

kaasneb osade funktsionaalsuste piiramatu kasutamine ning integratsioon väliste teenustega (näiteks Slack, Google Gmail, Google Drive).

Kolmas pakett on nimega Business, mõeldud suuremate tiimide haldamiseks ja maksab 19,50 eurot kuus ühe liikme kohta {aastakaupa makstes; kuukaupa makstes on ühe kuu tasu 23,50 eurot). Paketi Plus võimalustele lisanduvad siin privaatsed meeskonnaruumid, turvaline ainulogimisega juurdepääs ning lisandub integratsioon väliste teenustega (nt Github, Gitlab, Asana).

Viimase paketi nimi on Enterprise. See on mõeldud suurtele firmadele ning selle puhul on vaja küsida konkreetset pakkumist. Lisaks Business paketi võimalustele lisanduvad siin võimalused kasutajate täpsemaks haldamiseks, logide seireks ja oma domeenide haldamiseks.[12].

Notioni 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 Notioni kasutamise osas.

Soovitus: kontrollida toote hinnakirja ning lisanduvaid kulusid

EL/NATO liikmesriigis hoitavad andmed

Teenuse andmiseks kasutab Notion Amazon Web Services (AWS) (jms) andmekeskusi ja teenuseid, mis asuvad Ameerika Ühendriikides ja Saksamaal[13].

GDPR-i kohaselt võib andmeid edastada väljapoole Euroopa Liitu kui on rakendatud asjakohased kaitsemeetmed (artikkel 46[14]).

Andmete asukoht sõltub seega teenuse infrastruktuurist ja Notioni ning AWSi serverite asukohtadest.

Soovitus: kontrollida, kus andmeid majutatakse ja varundatakse

Teenusest lahkumise ja andmete ekspordi võimalus

Kliendiandmetest tehakse iga minuti järel uus varukoopia. Kui klient on kogemata mõne lehe, tööala või konto kustutanud, saab võtta ühendust Notioniga (emailiga team@makenotion.com) ning neil on võimalik taastada kaduma läinud info. Selle tegemiseks on aga maksimaalselt aega 30 päeva. See käib ka genereeritud sisu ja vektorkujutiste (embedding) kohta.

Klientidel on võimalus ise andmeid varundada ja eksportida. Andmete eksportimiseks on kasutusel vormingud PDF, HTML ja Markdown & CSV. HTML ja Markdown & CSV puhul on võimalik ühte eksporti kaasata kõik alamlehed. PDF ekspordi puhul saab kõik alamlehed eksportida Business või Enterprise pakettide puhul. Oluline on märkida, et kui klient on ise eksportimisega oma andmed varundanud, siis eksporditud faile üles laadides pole võimalik tööala koheselt taasluua. Tööala või lehe taastamiseks on ikkagi vaja ühendust võtta Notioniga.[15]

Notionil on ulatuslik varundusprogramm ning nad testivad pidevalt oma taasteplaane ja jätkuvusplaani (business

[12] https://www.notion.com/pricing

[13] https://www.notion.so/notion/Notion-s-List-of-Subprocessors-268fa5bcfa0f46b6bc29436b21676734

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

[15] https://www.notion.com/help/back-up-your-data

continuity program)[16]. Kliendiandmed varundatakse kord päevas erinevatesse andmekeskustesse, varukoopiad on krüpteeritud sarnaselt tootmisandmetele (production data)[17].

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

Soovitus: andmete kustumise korral võtta ühendust teenusepakkujaga 30 päeva jooksul

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

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid[18].

Notionil on neli ISO sertifikaati: ISO 27001, ISO 27701, ISO 27017 ja ISO 27018. Nad on läbinud SOC 2 Type 2 auditi American Institute of Certified Public Accountants (AICPA) poolt. Nad jälgivad German Federal Office for Information Security poolt loodud turvastandardit BSI C5 (Cloud Computing Compliance Controls Catalogue). Samuti on võimalik Notioni keskkonda üles seada nii, et see oleks vastavuses HIPAA (The Health Insurance Portability and Accountability Act) nõuetega. Nad osalevad ka DPF (Data Privacy Framework) programmis.[19] [20]

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[21].

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)[22]. 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

[16] https://www.notion.com/security
[17] https://www.notion.com/help/security-and-privacy
[18] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[19] https://www.notion.com/help/hipaa
[20] https://www.dataprivacyframework.gov/list
[21] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[22] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

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 [23].

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[24].

Soovitus: kontrollida, kas olemasolevad sertifikaadid on vastavuses KüTS nõuetega

Andmekaitse meetmete rakendamine

Andmetöötlust reguleerivad peamiselt teenuseleping (Master Subscription Agreement)[25] ja andmetöötluslisa (Data Processing Addendum)[26]. Sõltuvalt kasutatavatest teenustest võivad kohalduda täiendavad tingimused[27]. Notioni veebilehel on leitav ka privaatsuspoliitika (Privacy Policy)[28], kuid puudub selgus, kuidas see suhestub teenuselepingu ja andmetöötluslisaga.

Notion seab teenuselepingus piirangud, milliseid andmeid võib Notioni teenuses kasutada. Notionis ei või töödelda terviseandmeid, kui ei ole teisiti kokku lepitud, krediitkaardiandmeid ning andmeid, mis on vastuolus Notioni kasutus- ja sisu poliitikaga (Notion's Use and Content Policy).

Ka andmetöötluslisa esitab täpsustusi, mida kliendi isikuandmed sisaldada ei tohi. Sellega laiendab andmetöötluslisa teenuselepingus välja toodud nimekirja. Üldiselt ei tohi kliendi isikuandmed sisaldada tundlikke isikuandmeid (sensitive personal data). Mh ei tohi kliendiandmed näiteks sisaldada biomeetrilisi andmeid ega valitsuse väljastatud identifikaatoreid. Teenuseleping sisaldab üldist konfidentsiaalsusklauslit.

Pärast teenuselepingu lõppu teeb Notion kliendile 30 päevaks kättesaadavaks kõik kliendiandmed (Customer Data). Selle perioodi möödumisel võib Notion kõik kliendi andmed kustutada.

Andmetöötluslisa kohaselt peab Notion teenuselepingu lõppemisel kliendi nõudmisel kõik kliendi isikuandmed kliendile tagastama või turvaliselt hävitama (välja arvatud varunduse või arhiveeritud koopiad, mis kustutatakse Notioni andmete säilitamise kava (Notion' data retention schedule)) kohaselt. See ei kohaldu, kui Notion peab andmeid säilitama seadusest tulenevalt.

[23] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[24] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[25] https://www.notion.so/notion/Master-Subscription-Agreement-4elc5dd3e3de45dfa4a8ed60fla43da0
[26] https://www.notion.so/notion/Data-Processing-Addendum-36lb540101274blfa7el6b90402b0d99
[27] https://www.notion.so/notion/Terms-and-Privacy-28ffdd083dc3473e9c2da6ec0llb58ac
[28] https://www.notion.so/notion/Privacy-Policy-3468dl20cf614d4c90J

Notion võib edastada andmeid rahvusvaheliselt, sh kolmandatesse riikidesse. Üldjuhul kasutab Notion selleks standardseid andmekaitseklausleid (Standard Contractual Clauses).

Notion teavitab klienti turvaintsidendist põhjendamatu viivituseta[29].

Notion on oma veebilehel avaldanud, et kliendid vastutavad ise enda poolt loodud andmete eest[30].

Enterprise paketi kasutajate puhul Notioni alltöötlejad ei talleta kasutajate tööala andmeid. Mitte Enterprise paketi kasutajate tööala andmeid võivad alltöötlejad enne kustutamist säilitada kuni 30 päeva.[31]

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, milliseid andmeid tootega töödeldakse

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 tuvastada, et see on loodud tehisaru abil. Organisatsioon peab näitama, kuidas tagatakse tehisaru reeglipärane kasutus.

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).

Notioni sisu- ja kasutuspoliitikas (Content and Use Policy)[32] on kirjas keelatud sisu ja tegevused:

- ebaseaduslik tegevus;
- kahjulik sisu;
- laste ärakasutamine;
- ahistamine, kiusamine, laimamine, ähvardused;
- vihakõne;
- intellektuaalomandi rikkumine;
- pahatahtlikud ja petlikud tegevused;
- privaatsuse rikkumine;
- teenuste häirimine;
- häkkimine;
- andmete kogumine spämmides;
- volitamata kommertssisu saatmine.

Sisu- ja kasutuspoliitikas[33] on ka kirjas eraldi reeglid just Notion AI kasutamise osas. Tehisintellekti ei või kasutada:

- kõrge riskiga kasutusjuhtudeks;
- eksitavateabe levitamiseks;
- poliitilisteks kampaaniateks;
- petlikeks tegevusteks;
- õiguslikuks, meditsiiniliseks või finantsnõustamiseks.

Notion AI lisatingimustes (Notion AI Supplementary Terms)[34] on defineeritud

[29] https://www.notion.so/notion/Data-Processing-Addendum-36lb540101274blfa7el6b90402b0d99

[30] https://www.notion.com/help/security-and-privacy

[31] https://www.notion.com/help/notion-ai-security-practices

[32] https://www.notion.so/notion/Content-Use-Policy-lb9a773d5583486cb5cld39a8d777a55

[33] https://www.notion.so/notion/Content-Use-Policy-lb9a773d5583486cb5cld39a8d777a55

[34] https://www.notion.so/notion/Notion-AI-Supplementary-Terms-fa9034c8b5a04818a6baf3eac2adddbb

täiendavaid tingimusi, mis otstarbel ei tohi Notioni mudeleid kasutada:

- mudelite arendamiseks, mis võiksid konkureerida Notion Alga;
- esitada Notion AI genereeritud väljundit inimese looduna;
- valimiskampaaniate ajal sisu levitamiseks;
- viisil, mis eirab tehnilist dokumentatsiooni, kasutusjuhiseid või parameetreid.

Notion rõhutab, et nende mudelid ei ole mõeldud selleks, et teha automaatselt otsuseid kasutajate eest ära. See on ikkagi mõeldud kasutaja abistamiseks ja tema töö kiirendamiseks.[35]

Kliendi vastutusala on kasutajate paroolide turvalisus, kasutajate juurdepääsud, andmekasutuspoliitika järgimine, seadistused välise sisuga töötamise kohta[36].

Kasutaja on oma andmete kontrollija, teisisõnu, kasutaja vastutab oma andmete loomise, kasutamise, säilitamise, töötlemise ja kustutamise eest.[37]

Soovitus: kontrollida, et toodet ei kasutataks keelatud viisidel

Turvameetmete rakendamine

Krüpteeritud on nii jõudeolekus andmed (AES- 256} kui liikvel andmed (vähemalt TLS 1.2). Kliendi andmed on krüpteeritud ka varukoopiates, andmebaasitabelites, pilvtalletuses, ettevõtja sisevõrgus. Ka alltöötlejatele andmete edastamiseks kasutatakse TLS 1.2+ protokolliga kaitstud sidekanalit[38].

Notion kasutab kolmanda osapoole võtmehaldusteenust (Key Management Service, KMS}, millega automaatselt hallatakse võtmete loomist, pääsukontrolli, turvalist salvestamist, varundamist ja võtmete perioodilist vahetamist. Krüptovõtmed on määratud konkreetsetele rollidele minimaalõiguste põhimõtte järgi ning võtmeid uuendatakse automaatselt kord aastas. Võtmete kasutamist jälgitakse ja logitakse.

Kliendiandmed ei asu kunagi väljaspool tootmisekeskkonda. Erinevate klientide andmed on üksteisest loogiliselt eraldatud.

Business ja Enterprise klientidele pakutakse ainulogimise võimalust (SSO}. Kaksikautentimine (2FA} on võimalik seadistada kõigil klientidel. Samuti on tööalade omanikel (workspace owners} võimalik õiguste seadmise kaudu reguleerida kasutajate juurdepääsu sisule.

Pöördumised kriitiliste süsteemide suunas logitakse ja logid kogutakse kesksesse SIEM süsteemi. Tööalade omanikud (workspace owners} saavad juurdepääsu turvalisuse ja ohutusega seotud liiklusinfole.

Võimalik on teenus liidestada kliendi DLP ja SIEM lahendustega[39]. AWS andmekeskuste füüsilise turvalisuse korraldab AWS.

Kliendi - ja süsteemiandmed varundab Notion iga päevaselt, erinevatesse andmekeskustesse. On olemas taasteplaan (disaster recovery plan}, mida testitakse kord aastas, ja jätkuvusplaan (business continuity plan}.

Uuenduste projekteerimisel ohud modelleeritakse ja tarkvara disain vaadatakse läbi turvalisuse seisukohast,

[35] https://www.notion.com/help/ai-safety
[36] https://www.notion.com/help/how-notion-protects-against-prompt-injection-risks
[37] https://www.notion.com/help/security-and-privacy
[38] https://www.notion.com/help/notion-ai-security-practices
[39] https://www.notion.com/help/add-security-and-compliance-integrations

samuti vaadatakse läbi loodud kood ja turvatestitakse see enne avalikustamist.

Nõrkuste otsingut teostatakse nii tootel kui kõigil taristuga seotud hostidel. Kõigil avalikel otspunktidel kasutatakse tulemüüri. Teenustõkestusrünnete vastu kasutatakse kolmanda osapoole lahendust. Toimib veaotsingu tasuprogramm.

Ettevõttes on rakendatud korralduslikud turvameetmed, olemas on intsidendihaldusplaan. Sisemine turvaaudit viiakse läbi vähemalt kord aastas. Kus võimalik, nõuab Notion oma töötajalt ta mitmikautentimist (MFA}. Ettevõttesiseselt kehtib minimaalõiguste printsiip: juurdepääsu saavad vaid need töötajad, kel see töökohustusteks vajalik on. Pääsuõigused vaadatakse regulaarselt üle. Kasutusel on kolmanda osapoole EDR-tehnoloogia.

Leitud AI nõrkused: Septembris 2025 näidati võimalust manipuleerida Notion AI agenti tundlikku infot lekitama[40], millele Notion reageeris kiiresti, lisades lisakontrollimehhanismi nii kasutajatele kui administraatoritele[41]. Varasemast on teada koodi kaugkäitusnõrkus[42].

Ettevõte lubab, et arendab Notion AI'd vastutustundlikult ja turvaliselt, vaatab regulaarselt üle oma AI ohutusmeetmed, on Notion AI arendamise, juurutamise ja kasutamise osas läbipaistev, informeerides kasutajaid sellest, milliste tootjate mudeleid kasutatakse.

Notion kasutab alltöötlejaid. Alltöötlejate nimekiri on leitav nende veebilehelt. Kliendil endal on võimalik seadistada, kas ta soovib, et tema andmeid kasutataks Notion AI parendamiseks[43].

Vaikeväärtusena on mudelite treenimine kasutajaandmetega välja lülitatud. Mudeli väljundi ohutuse tagamiseks rakendab Notion meetmeid nagu OpenAI moderation endpoint.

Notion testib oma mudeleid enne kasutajate kätte andmist regulaarselt. Olemas on põhjalikud infoturbe- ja privaatsuskavad (privacy program}. Samuti kontrollitakse regulaarselt kliendiandmete alltöötlejaid (nt OpenAI}[44].

Kliendiandmete vektoresitusele (embedding} seab Notion sama kõrged turvalisuse ja privaatsuse nõuded kui kliendiandmete kaitsele[45]. Dokumentides Master Service Agreement (MSA} ja Data Processing Agreement (DPA} kliendiandmete kohta sätestatu kehtib ka kliendiandmete vektoresituse kohta. Vektoresitusi hoitakse Turbopufferi andmebaasis, mis on läbinud SOC 2 Type 2 auditi.

Notioni andmetöötluslisa täpsustab piiranguid, mida Notion kliendi isikuandmetega teha ei või[46]. Notion ei tohi kliendi isikuandmed (Customer Personal Data} müüa, jagada ega töödelda käitumispõhise või sihitud reklaami ("cross-context behavioral advertising" or "targeted advertising"} tarbeks, töödelda muul eesmärgil kui kliendiga kokkulepitud ärilisel eesmärgil.

Vastuste genereerimisel lähtub Notion AI kasutaja kehtivatest pääsuõigustest: vastused genereeritakse ainult selle teabe pealt, millele kasutajal on juurdepääs.

Kliendi andmed on eraldatud teiste klientide andmetest, AI ei töötle neid kunagi koos.

Enterprise klientidel on võimalik oma sisu (sh AI promptide sisu ja genereeritud sisu}

[40] https://forum.gnoppix.org/t/notion-3-0-s-new-ai-agents-can-be-tricked-into-leaking-data-through-a-malicious-pdf/1651
[41] https://the-decoder.com/notion-ai-agents-get-security-update-after-data-leak
[42] https://socradar.io/labs/app/eve-radar/CVE-2024-23743
[43] https://www.notion.com/help/notion-ai-faqs
[44] https://www.notion.com/help/ai-safety
[45] https://www.notion.com/help/notion-ai-security-practices
[46] https://www.notion.so/notion/Data-Processing-Addendum-36lb540101274blfa7el6b90402b0d99

kaitsta kogemata kustutamise vastu, lüitades sisse andmekaotõrje (data loss prevention (OLP)}[47].

Kuna Notion AI agent suudab sisendit lugeda kogu veebist, kasutaja sisust ning ühendatud teenustest (apps}, on oht promptisüstide (prompt injection} rünneteks suur. Selles kontekstis räägib Notion jagatud vastutusest (vt kliendi kohustused}, omalt poolt lubab, et üleslaetud failidest tuvastatakse peidetud kasud tõhusalt; lubab pidevat turvatestimist, agendi kõigi tegevuste logimist (sh välise sisuga tehtavad toimingud}, annab kliendi administraatorile võimaluse veebiotsing täiesti välja lülitada või seadistada kinnituse küsimine, kui agent külastab veebilehte. Kasutajatele on juhis tööala turvaliseks kasutamiseks[48].

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.

[47]https://www.notion.com/help/notion-ai-security-practices

[48]https://www.notion.com/help/how-notion-protects-against-prompt-injection-risks

AI-ga seotud riskid	
	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

Notion on rakendanud rohkeid infoturbe ja andmekaitse alaseid meetmeid, millega saab lugeda Notioni teenus usaldusväärseks. Notion majutab andmeid Ameerika Ühendriikides või AWS serveritel (pole teada täpne asukoht), millega ei ole tagatud andmekaitsenõuete täitmine.

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

Vajalik on rakendada täiendavaid meetmeid paralleelselt Notioni kasutamisega, mh koolitada kasutajaid, arendada alternatiivseid töömeetodeid, kontrollida Notionile 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 Notion sobiv kasutamiseks. Arvesse tuleks võtta AI kasutamisega ja pilvtoodetega seonduvaid riske ning Notioni poolt rakendatud meetmeid turvalisuse tagamiseks.