

Chat GPT

Kirjeldus

Käesolev usaldusväärse hinnang keskendub OpenAI ChatGPT pilvtöötlusteenuse (edaspidi ChatGPT) 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 tavatariibile kättesaadavamaks muutumine on põhjustanud selles valdkonnas arenguhüppe, sealhulgas AlaaS (artificial intelligence as a service, tehisintellekt teenusena) ärimudeli leviku.

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

OpenAI on üks maailma juhtivaid asutusi tehisarutehnoloogiatega uurimise ja arendamise valdkonnas. OpenAI, Inc. rajati 2015. aastal mittetulundusliku organisatsioonina, kuid on tänaseks kasvatanud enda alla keerulise struktuuriga korporatsiooni, mille ühes harus

tegutsevad ka kasumit taotlevad ettevõtted nagu ChatGPT teenustaja OpenAI OpCo, LLC ja selle allharu OpenAI Ireland Ltd Euroopas.

ChatGPT turuletoomine 2022. aasta novembris pani alguse generatiivsete tehisarutehnoloogiatega buumile, mis innustas suuri tehnoloogiaettevõtteid (Microsoft, Google, Meta jt) suunama järsult rohkem ressursse oma tehisarulistele vestlusrobotite turuletoomisse. ChatGPT jõudis 100 miljoni kasutajani kõigest kahe kuuga, mis tegi sellest kõige kiiremini sellise tähiseni jõudnud tarkvara ajaloos¹.

Tänini on tegu absoluutse turuliidriga: teenusel on 700 miljonit kasutajat², moodustades nii enam kui 80% tehisaru vestlusrobotitele suunatud veebiliiklusest³. Ühtlasi on ChatGPTs pakutavad mudelid valdavalt liidrid ka erinevate parameetrite alusel koostatud järjestustabelites, mis hindavad mudelite kvalitatiivseid ja kvantitatiivseid võimeid^{4,5}.

Ettevõtte ja teenuse jätkusuutlikkuse osas kindlus puudub. Kuigi ChatGPT-d teenustava ettevõtte käive kasvab jõudsalt (2023. a 1,6 mld dollarit, 2024. a 5,5 mld dollarit ja 2025. a esimese seitsme kuuga 12,0 mld dollarit), siis suurte käituskulude ja jätkuvate investeringute tõttu on

¹<https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>

²<https://www.cnbc.com/2025/08/04/openai-chatgpt-700-million-users.html>

³<https://gs.statcounter.com/ai-chatbot-market-share>

⁴<https://artificialanalysis.ai/leaderboards/models>

⁵<https://www.vellum.ai/llm-leaderboard>

rahavoog olnud tugevalt negatiivne kogu tegutsemise vältel⁶.

Kasumlikkuseni ettenähtavas tulevikus samuti ei jõuta, sest keskendutakse investorite finantseerimise toel tehnoloogia arendamisele ja kasutajaskonna kasvatamisele⁷. Eksisteerib risk, et kapitali pealevool OpenAI-le hakkab vähenema või lõppeb sootuks, kui ettevõtte ei suuda investorite ootusi neile aktsepteeritava perioodi jooksul täita. Investorite ootusi ja kapitalipaigutuse otsuseid mõjutavad

Teenuse võimalused

SaaS - olemuselt on ChatGPT teenustaja pilvetaristul töötav virtuaalne assistent, mida saab kasutada nii veebisirvijas kui ka mobiiliseadme rakenduses. ChatGPT vestlusrobot annab vastuseid kasutaja antud sisendi ja korralduste ajal üksikute käsundite (promptide) kaupa.

ChatGPTd 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 keeleti varieerub, sõltudes keelemudeli treenimisel kasutatud konkreetse keele korpuse mahust.
- Vastab sidusas ja korrektses keeles, liigendab ja vormindab vastustekstid inimlugejale hõlpsasti loetavaks.
- Arvestab vastustes sama vestluse varasemat konteksti.
- Sõnastab vastused kasutaja soovidest lähtuva tonaalsuse,

omakorda kiiresti arenevad sündmused AI-sektoris laiemalt. Valdkonnas tegutsevate ettevõtete bilansid on omavaheliste ringtehingute mõjul üles paisutatud ega peegelda enam adekvaatselt nende tegelikku vaartust⁸. Asjatundjate sõnul on tegu nn finantsmulliga, mille võimalik lõhkemine tooks kaasa järske hairinguid AI-teenuste turul, sh teenustajate pankrotte ja teenuste sulgemist.

OpenAI volitatud töötajate osas eraldi usaldusväärse hinnangut ei koostata ja usaldatakse teenusepakkujat.

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 vestlusroboteid (nn GPTsid), mis vestlevad ja täidavad korraldusi kasutaja määratletud eeskirjade raames ning kasutaja antud teabe põhjal ja kontekstis.
- Kasutaja loal ühendub tema pilvteenuse kontodega (connectors), et töödelda käsundite täitmisel neis sisalduvaid andmekogumeid (märkmeh, kalendrissekkanded, e-kirjad, sõnumid, andmetabelid, tekstidokumendid, pildid, programmikood jms); hetkel ühildub 23 pilvteenusega⁹.

ChatGPT'I on järgmised spetsiifilised võimed:

⁶<https://www.reuters.com/business/media-telecom/openais-annualized-revenue-hits-10-billion-up-55-billion-december-2024-2025-06-09>

⁷<https://www.cnbc.com/2025/09/06/openai-business-to-burn-115-billion-through-2029-the-information.html>

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

⁹<https://chatgpt.com/features/connectors/>

- 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.
- Genereerib ideid.
- Koostab loome- ja tarbetekste (luuletusi, jutustusi, reklaamtekste, juhendeid, teabelehti jms).
- Otsib Internetist teavet ja annab viited.
- Suudab tõlgendada ja kirjeldada ette antud 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 paljude teabeallikate põhjal. Teeb kasutaja eest toiminguid Internetis (agent), sh kasutaja kontodel pilvteenustes, mis on ChatGPT-ga ühendatud; toimingutes, mis nõuavad autentimist või kinnituse andmist, tuleb kasutajal ise sekkuda (nt makse tegemine või e-kirja saatmine).

Ülaltoodud võimete realiseerimise võimalus, kiirus ja kvaliteet sõltub keelemudelist, mida kasutaja käsundi täitmiseks rakendatakse.

EL tehisintellekti määruse kohane riskitase

ChatGPT teenust vaatleme kui hulka üldotstarbelisi suuri keelemudeleid, mida kasutatakse vestlusroboti teenuse

Keelemudelid, mida ChatGPT pakub, on¹⁰

- GPT-5;
- GPT - 5 thinking;
- GPT-5 pro;
- GPT - 5 thinking mini;
- GPT-4o;
- GPT-4.1;
- GPT-4.5;
- OpenAI o3;
- OpenAI o3 pro;
- OpenAI o4-mini.

Mistahes keelemudeliga koos töötavad ka graafilist väljundit loovad mudelid, mis käivituvad vastava korralduse peale vestluses:

- GPT Image 1 - redigeerib ja loob uusi kujutisi etteantud kujutiste põhjal;
- DALL- E - loob kirjelduse põhjal kujutisi;
- Sora - loob kirjelduse põhjal videoklippe.

OpenAI on teenuste seisu lehekülj¹¹, kus antakse ülevaade pakutavate teenuste hetkeseisust. Teenuse aktiivajaks (uptime) näitas lehekülj vaatamise hetkel 99,50%, kuid pole märgitud, millise perioodi lõikes on see näitaja arvatud.

Avalikus teenuslepingus¹² sätestab OpenAI, et teenust antakse saadaoleva ressursi piires (as is) ning ütleb lahti kohustusest ja vastutusest tagada klientidele mistahes määral teenuste talitluspädevust (punkt 12.2).

Konkreetset teenusetasemelepingut, milles võiks teenustaja võtta endale kohustuse määratletud käideldavuse taseme tagamiseks, pakutakse kõrgeima taseme äriklientidele (Enterprise pakettis).¹³

¹⁰<https://chatgpt.com/pricing/>

¹¹<https://status.openai.com/>

¹²<https://openai.com/policies/services-agreement/>

¹³<https://chatgpt.com/pricing/>

kirjeldatud töölusjuhule klassifitseerub piiratud riskiga tehisintellektiks.

ChatGPT-d on võimalik kasutada ka viisidel, mis klassifitseeriks 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 üksiku ametniku (ChatGPT kasutaja) tasemel.

Kuna tehisaru vestlusrobotid, ja hetkel eelkõige ChatGPT, on laialt levinud ka eratarvitusel, siis on oluline rõhutada, et kõik käesolevas hinnangus käsitletud

asjaolud kohalduvad vaid ärikliendi kontoga soetatud litsentsidega teenust kasutades. Eratarbijale mõeldud (tasuta ja tasulised) ekvivalentsed OpenAI teenused, mida tarvitsevad regulaarselt kasutada ka litsentse omavate asutuste töötajad, alluvad teistsugustele tingimustele. On oluline, et töötajad kasutaksid tööalase teabe töötlemiseks asutuse litsentsiga ChatGPT kontot, isikliku teabe töötlemiseks aga oma eralitsentsiga seotud kontot.

ChatGPT teenuse mudelid, omadused ja teenusetingimused arenevad kiiresti. Seepärast tuleb kasutuselevõtjal hoida end jooksvalt kursis sellega, mis on kirjas OpenAI Privacy Portalis¹⁴.

Soovitus: kontrollida, et toodet kasutatakse lubatud viisil

Kasutusjuhud

Peamiselt leiab ChatGPT kasutust järgmistes toimingutes:

- nõuandvad vestlused, abi otsuste tegemisel;
- ideede genereerimine;
- reklaam - ja tarbetekstide koostamine;
- tekstide toimetamine;
- tekstide tõlkimine;
- teabe (faktide) ja seletuste küsimine;
- etteantud materjalide tõlgendamine, neist kokkuvõtete tegemine või konkreetse teabe ülesleidmine;
- programmeerimine;
- visuaalide genereerimine.

Läbi ChatGPT kasutajaliidese on võimalik kasutada toodet järgmistel eesmärkidel:

Rahaline mõju

OpenAI pakub äriklientidele ChatGPT teenust kolmes kategoorias¹⁵.

Väiksema võimekomplektiga Business (endine Team) pakett maksab kasutaja

- saamaks abi 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;
- abi programmeerimisel (koodi kirjutamine).

Selline kasutusviis on asutuse tööprotsessidega seotud vaid kaudselt.

kohta 29 dollarit kuus (tasumine toimub kord aastas).

Suurema võimekomplektiga on Enterprise pakett, mille hind pole avalik.

¹⁴<https://privacy.openai.com/policies?name=welcometoopenai-privacy-portal>

¹⁵<https://chatgpt.com/pricing/>

Hinnapakkumise saamiseks peab ettevõtte või asutus tegema OpenAI-le päringu ChatGPT kodulehe kaudu. Eelduste kohaselt kujuneb hind lähtuvalt kasutajate potentsiaalsest arvust ja spetsiifilistest võimevajadustest. Avalikud allikad viitavad sellele, et hind võiks jääda 60 dollari (ligikaudu SOC) ringi kasutaja kohta kuus.

Sealjuures oli mitmes allikas väidetud, et minimaalne kasutajate arv peaks olema 150 ja lepingu kestus 12 kuud¹⁶.

Valitsusasutustele on mõeldud võimekomplekt ChatGPT Gov, mida pakutakse hetkel vaid USA valitsusasutustele.

Soovitus: kontrollida toote hinnakirja sobiva teenuse valimiseks ning lisanduvaid kulusid

EL/NATO liikmesriigis hoitavad andmed

ChatGPT teenuses töödeldavaid andmeid hoiab OpenAI mitme alltöötleja pilvetaristus paljudes riikides¹⁷:

- Microsoft Corporation: Austraalia, Kanada, Prantsusmaa, Saksamaa, India, Jaapan, Norra, Paola, Singapur, Lõuna-Aafrika Vabariik, Lõuna-Korea, Rootsi, Šveits, Araabia Ühendemiraadid, Ühendkuningriik, Ameerika Ühendriigid;
- CoreWeave, Inc: Norra, Hispaania, Rootsi, Ühendkuningriik, Ameerika Ühendriigid;
- Oracle Cloud Infrastructure: Brasiilia, Jaapan, Malaisia, Holland, Ameerika Ühendriigid;
- Google Cloud Platform: Jaapan, Holland, Norra, Ühendkuningriik, Ameerika Ühendriigid.

OpenAI ei ole määratlenud andmete hoidmise vaikeriiki ega täpsusta, kas ja

kuidas sõltub andmete paigutus ülaltoodud riikidesse klientide asukohast.

OpenAI pakub võimalust ChatGPT klientidel oma andmete hoidmise kohta valida, ent seda vaid Enterprise paketi kasutajatele¹⁸. Business paketi klientidele pole loodud OpenAI poolt ühtki ametlikku mehhanismi, et oma andmete töötlemise ja talletamise asukohta teada saada ja/või seda muuta.

Kõik Euroopa majanduspiirkonnas asuvad kliendid sõlmivad oma teenuslepingu ChatGPT kasutamiseks OpenAI lirimaa harukontoriga. Sealsete klientide andmete töötlemiseks võtab OpenAI kohustuse teha seda vastavuses Euroopa isikuandmete kaitse Üldmaarusega (GDPR) ning Euroopa Liidu standardsete andmekaitseklauslitega (SCC), sõltumata riigist, kus andmeid töödeldakse (andmetöötluste lisa: preambul, jaotised 1 ja 7)¹⁹.

Soovitus: valida pakett, mille korral on võimalik andmete asukohta valida

Teenusest lahkumise ja andmete ekspordi võimalus

Kui ChatGPT erakliendi pakettides on menüüs funktsioon oma andmete eksportimiseks, siis ärikliendi pakettides seda funktsiooni ei pakuta. Ise pilvteenuses saab klient oma andmeid süsteemist välja võtta vaid teksti „käsitsi“ kopeerides ja faile

salvestades²⁰. Teisalt võiks Euroopa Liidu andmekaitse Üldmääruse (GDPR) artiklile 20 viidates eeldatavasti olla võimalik oma andmeid teenustajalt välja nõuda. See protsess kirjaliku nõude esitamisest kuni andmete kättesaamiseni ei pruugi aga olla

¹⁶https://explodingtopics.com/blog/chatgpt-enterprise?utm_source=chatgpt.com/

¹⁷<https://openai.com/policies/sub-processor-1st/>

¹⁸<https://openai.com/business-data/>

¹⁹<https://openai.com/et-EE/policies/data-processing-addendum/>

²⁰<https://help.openai.com/en/articles/8801890-can-i-migrate-or-merge-my-personal-chatgpt-workspace-over-to-my-chatgpt-business-workspace>

sirgjooneline, sest teenustaja ise pole vastavat protseduuri kirjeldanud.

Ühtlasi ei võimalda ärikliendi pakettid ka andmete ennistamist. Näiteks rätsepkohaldusega GPTde parameetreid ei saa süsteemist välja viia (punkt 4.1). Teenuselepingus on sätestatud, et klient säilitab omandiõigused sisestatud andmetele ja on kõigi väljundandmete omanik. GPT-de parameetrite häälestamiseks loodud seadeid sisendandmetena ei käsitleta. Teenuselepingus on sätestatud, et kui klient katkestab ChatGPT teenuse kasutamise, kustutab OpenAI kliendi andmed 30 päeva pärast teenuse lõpetamist (punkt 11.3)²¹.

Avalikes allikates ei leidunud infot kliendiandmete varundamise kohta.

Soovitus: valida pakett, mis võimaldab andmete varundust ja eksporti

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

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid²⁷.

OpenAI-l on mitmeid sertifikaate ja auditeerimistöendeid, sh ISO/IEC 27001:2022 (kehtiv kuni 07.08.2028), CSA STAR, SOC 2, SOC 2 Type 11, SOC 3. Teisalt on teenustaja edukalt läbinud SOC 2 Type II auditi²⁸. Selle üks viiest hindamiskriteeriumist on piisavalt kõrge tõhususega meetmed käideldavuse tagamiseks. SOC 3 Type II auditi raportist²⁹ nähtub OpenAI tugev sõltuvus teistest pilvteenustest (Microsoft Azure, Snowflake, Okta ja WorkOS).

²¹<https://openai.com/policies/services-agreement/>

²²<https://www.reuters.com/business/openai-spend-100-billion-over-five-years-backup-servers-information-reports-2025-09-19/>

²³<https://help.openai.com/en/articles/7260999-how-do-i-export-my-chatgpt-history-and-data>

²⁴<https://medium.com/@flyingfathead/help-openai-chatgpt-team-plan-just-took-all-of-my-data-as-hostage-06f8dc8335eb>

OpenAI lähema viie aasta plaanitud kulutused varundusserverite rentimiseks pilvteenuste pakkujatelt on märkimisväärsed²².

Erakasutajal on võimalik oma vestluste ajalugu ja andmed eksportida²³, aga Business paketi kasutajal mitte²⁴. Assistenti loomisel üles laetud faile ei saa alla laadida²⁵.

Mudelite kaitseks on mitmeid meetmeid²⁶, ent nende varundamist otsesõnu ei väideta.

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

Business pakett ei kuulu ülaltoodud sertifikaatide ja auditite skooopi (v.a SOC 3 puhul). Valdavalt hõlmavad need ChatGPT Enterprise, ChatGPT Edu ja OpenAI AP/teenuseid.

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.

²⁵https://www.reddit.com/r/OpenAIDev/comments/lhl6mu5/is_there_a_way_to_download_files_from_an_openai/

²⁶<https://openai.com/index/securing-research-infrastructure-for-advanced-ai>

²⁷<https://www.ria.ee/sites/default/files/document/s/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>

²⁸<https://trust.openai.com/>

²⁹<https://trust.openai.com/?itemId=27a3eac6-90c8-402d-ald8-817e02eb07f0&source=title>

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 õigusraamistikku³⁰.

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)³¹. 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 andmetöötuse ja AI kasutamise eesmärk, millised andmetöötusprotsessid süsteemis toimuvad, millised andmed ja kelle vahel liiguvad ning millist AI-süsteemi või komponenti (sh selle riskitase) süsteemis kasutatakse³².

Standardite järgimine panustab toodete või teenuste ohutuse, kvaliteedi ja töökindluse tagamisse, samuti võivad need parandada ja tõhustada ettevõtte süsteeme või protsesse. AI süsteemide erinevate elutsükli etappide puhul rakendatavate standardite kohta on võimalik lugeda ENISA publikatsioonist heade küberturvalisuse praktikate kohta AI süsteemide puhul³³.

Soovitus: kontrollida alltöötajate vastavust standarditele ja KüTS nõuetele

Andmekaitse meetmete rakendamine

Andmetöötlust reguleerivad peamiselt teenuseleping (OpenAI Services Agreement)³⁴ ja andmetöötuse lisa (OpenAI on esitanud selle erinevates

keeltes, kuid puudub täpsustus, mis keelset versiooni tuleb vaidluste korral vaadata)³⁵.

Teenuseleping ja andmetöötuse lisa kasutavad termineid kliendisisu (Customer

³⁰<https://www.ria.ee/sites/default/files/document/s/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>

³¹https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

³²<https://www.ria.ee/sites/default/files/document/s/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>

³³<https://www.ria.ee/sites/default/files/document/s/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf>

³⁴<https://openai.com/policies/services-agreement/>

³⁵<https://openai.com/et-EE/policies/data-processing-addendum/>

Content) ja kliendi andmed (Customer Data). Kliendisiseks on kliendi (ja tema loppkasutajate) poolt sisestatud ja OpenAI teenuste poolt väljastatud andmed (Input and Output). Kliendi andmed on isikuandmed, mille klient on OpenAI-le andnud ning mida OpenAI töötleb kliendile teenuste osutamiseks.

Teenuselepingu kohaselt kasutab OpenAI kliendisise teenuste pakkumiseks, kohalduva seaduse järgimiseks, OpenAI poliitikate (policies) jõustamiseks ja väärkasutamise vältimiseks. OpenAI ei kasuta kliendisise teenuste arendamiseks, kui kliendiga ei ole teisiti kokku lepitud.

Klient peab tagama, et tal on kõik õigused, litsentsid ja load sisendandmete (Input) sisestamiseks teenusesse. Klient ise vastutab väljundandmete (Output) kasutamise eest ning nende õigsuse ja sobivuse hindamise eest.

Klient nõustub, et ta kaitstud terviseinfot (Protected Health Information) ei töötle, kui ta pole selleks sõlminud eraldi lisalepingut. Sellisel juhul ei tohi kaitstud terviseinfot OpenAI teenustes kasutada.

Teenuseleping sisaldab üldist konfidentsiaalsusklauslit. Teenuselepingu lõppemisel kustutab OpenAI 30 päeva jooksul kogu kliendisise oma süsteemidest, kui seadusest ei tulene teisiti või pole muud moodi kokku lepitud.

Kui klient kasutab teenuseid isikuandmete töötlemiseks, siis järgivad OpenAI ja klient andmetöötlaste lisa. Andmetöötlaste lisa kohaselt kohustub (NB! ingliskeelses tekstis on kasutatud sõna „agrees“) OpenAI töötlema kliendi andmeid ainult OpenAI teenuste pakkumiseks ja toetamiseks (sh ülevaadete, aruandluse, analüüsi, platvormi kuritarvituste ja ohutuse jälgimise eesmärgil).

OpenAI teavitab klienti isikuandmetega seotud rikkumisest teadasaamisest põhjendamatu viivitusega. Täpsemat aega ei ole kokku lepitud.

Klient kinnitab ja tagab, et tal on kõik vajalikud õigused, nõusolekud ja volitused,

et anda kliendiandmeid OpenAI-le ning lubada OpenAI-l kasutada, avaldada, säilitada ja muul viisil töödelda. Andmetöötlaste lisast ilmneb, et OpenAI võib andmeid edastada kolmandatesse riikidesse.

Andmetöötlaste lisa kehtib kuni OpenAI töötleb kliendi nimel kliendiandmeid või kuni teenuselepingu lõppemiseni (ja kuni kõik kliendi andmed on tagastatud või kustutatud). OpenAI säilitab API teenuse kaudu saadatud API kliendiandmeid maksimaalselt kolmkümmend (30) päeva, v.a kui õigusaktides on nõutud teisiti. ChatGPT Enterprise teenuse kliendi andmeid säilitab OpenAI lepingu kehtivuse ajal, kui lepingus või tellimisvormis ei ole sätestatud teisiti. Seejuures on OpenAI lisanud andmetöötlaste lisasse täpsustuse, et „OpenAI võib jätkata selliste kliendiandmete töötlemist, mis on mitteisikustatud, anonüümseks muudetud ja/või koondkujul nii, et andmeid ei loeta enam isikuandmeteks vastavalt kohaldatavatele andmekaitse seadustele ja viisil, mis ei võimalda OpenAI süsteemide ja teenuste arendamisel tuvastada üksikisikuid või klienti“.

OpenAI lehel on vorm andmetöötlaste lisa sõlmimiseks (<https://ironcladapp.com/public-launch/63ffefa2bed6885f4536d0fe>), kuid jääb ebaselgeks, kas selle vormi täitmata jätmisel andmetöötlaste lisa ei kohaldugi.

OpenAI kasutab alltöötlejaid. Alltöötlejate nimekiri on leitav veebilehelt: <https://openai.com/policies/sub-processor-list/>.

Juhul, kui ChatGPT-d ei kasutata ärikliendina, kohalduvad erakliendi teenusetingimused (<https://openai.com/policies/terms-of-use/>) ja privaatsuspoliitika (<https://openai.com/policies/privacy-policy/>). ChatGPT-l on esinenud probleeme

GDPR'i nõuete täitmisega³⁶. Euroopa Andmekaitse Nõukogu lõi ka töögrupi ChatGPT uurimiseks, mis on avaldanud raporti uurimise osas³⁷. Seega on vajalik põhjalik analüüs ja asutusesisese regulatsiooni loomine enne, kui ChatGPT'sse isikuandmeid sisestatakse. Ühtlasi peavad olema kasutusel meetmed, et vältida isikuandmete sisestamist, kui

asutuse otsus on isikuandmeid ChatGPT'sse mitte sisestada.

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, kuidas on andmekaitseenõuded tagatud

Erinõuded

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

Tehisaru poolt loodud sisu, näiteks pildid, heli või videofailid, tuleb selgelt sellistena märgistada - et selle sisu edasistel kasutajatel oleks võimalik tuvastada, et sisu on loodud tehisaru abil

Nõuded kasutuselevõtjale: 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).

ChatGPT teenuse kasutamisel tuleb järgida teenuse kasutamise reegleid³⁸. Teenust ei tohi kasutada järgmistes tegevustes ega eesmärkidel:

- isikute hirmutamiseks, ähvardamiseks, laimamiseks, ahistamiseks, enesetapule või enesevigastamisele õhutamiseks, toitumishäirete propageerimiseks;
- haavatavas seisundis isikute ärakasutamiseks;
- intiimse sisu töötlemiseks asjaomaste isikute nõusolekuta;
- vägivalda õhutamiseks;

- relvade väljatöötamiseks, hankimiseks ega kasutamiseks;
- ebaseaduslike kaupade loomiseks või teenuste pakkumiseks;
- teiste süsteemide või vara hävitamiseks või kahjustamiseks, sh kuritahtlikuks kübertegevuseks;
- intellektuaalse omandi õiguste rikkumiseks;
- pärisrahaga hasartmängudes;
- juriidiliseks või meditsiiniliseks nõustamiseks ilma litsentseeritud eksperdi kaasamiseta;
- riikliku julgeoleku tagamise või luure eesmärgil ilma OpenAI heakskiiduta;
- isikute kohta käiva tundliku teabe jälgimiseks, kogumiseks ega levitamiseks;
- isikute tuvastamiseks ega profileerimiseks;
- isikute imiteerimiseks, sh fotorealistlike piltide või hääletämbri taasloomiseks ilma asjaomaste isikute nõusolekuta;
- isikute hindamiseks ega klassifitseerimiseks nende sotsiaalse käitumise või isikuomaduste põhjal;
- järelduste tegemiseks isiku emotsioonide kohta töökohal ja hariduskeskkonnas, välja arvatud juhul, kui see on vajalik

³⁶<https://syrenis.com/resources/blog/chatgpt-gdpr/>

³⁷https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

³⁸<https://openai.com/en-GB/policies/usage-policies/>

- meditsiinilistel või ohutuslastel põhjustel;
- isiku kuriteo toimepanemise riski hindamiseks või ennustamiseks ainult tema isikuomaduste või profileerimise põhjal;
- alaealiste isikute ärakasutamiseks, ohustamiseks, seksualiseerimiseks, ahvatlemiseks, paljastamiseks, vanusele sobimatule sisule, välimuse või muude omaduste häbistamisele, ohtlikele väljakutsetele õhutamiseks, vanusepiiranguga kaupadele ja teenustele juurdepääsu tagamiseks;
- akadeemiliseks petmiseks;
- kelmusteks;
- rämpsposti tootmiseks ja saatmiseks;
- poliitiliseks kampaaniaks ega lobitöök;
- valimistesse sekkumiseks;

- kõrge riskiga automatiseeritud otsuste tegemiseks tundlikes valdkondades (kriitiline taristu, haridus, eluase, tööhõive, finantstegevus ja krediit, kindlustus, õiguskaitse, meditsiin, olulised valitsusteenused, tooteohutus, riiklik julgeolek, ränne), ilma et otsuse vaataks läbi inimene.

Ühtlasi nõustub klient teenust kasutama hakates, et ei töötle kaitstud terviseinfot (Protected Health Information), kui ta ei ole selleks eraldi lisalepingut sõlminud (teenuselepingu punkt 5.4³⁹).

Lähtuvalt teenuselepingust vastutab kasutatav organisatsioon ise teenusesse sisestatud andmete eest. Teatud tüüpi andmete sisestamine teenusesse on keelatud.

Soovitus: kontrollida, et teenust kasutatakse lubatud eesmärkidel

Turvameetmete rakendamine

Andmetöötluse lisas B⁴⁰ ning Enterprise, Business, Edu ja API pakettide andmekaitse ja turvalisuse veebilehel⁴¹ on kirjeldatud nii korralduslikud, personali, füüsilise turvalisuse kui ka tehnilised turvameetmed riist- ja tarkvara, andmekeskuste ja võrkude, juurdepääsu, seire ja logimise, nõrkuste ja rikete tuvastamise, intsidentidele reageerimise, krüpteerimise, riskihalduse (sh kolmandate osapoolte osas), turvahindamiste jms osas.

AI-taristu turvalisuse osas pakkus OpenAI välja kuus uut, spetsiifiliselt AI-taristu turbeks mõeldud meedet⁴², mida vähemalt ChatGPT puhul ei ole siiani rakendatud.

Turvameetmeid, millega kaitstakse OpenAI esindusmudelite (frontier models) arendustöök kasutatavate superarvutite turvalisust, on kirjeldatud⁴³, erilist rõhku pannakse mudeli konfidentsiaalsuse hoidmisele, aga ka turvalisust toetava arhitektuuri kirjeldamisele.

OpenAI API, Enterprise, Teams (nüüd Business) ja Edu pakettide turvameetmeid kajastab ka CAIQ enesehindamine⁴⁴.

OpenAI nõuab oma tarnijatelt (suppliers) infoturbekava järgimist⁴⁵.

³⁹<https://openai.com/policies/services-agreement/>

⁴⁰<https://openai.com/et-EE/policies/data-processing-addendum/>

⁴¹<https://openai.com/business-data/>

⁴²<https://openai.com/index/reimagining-secure-infrastructure-for-advanced-ai/>

⁴³<https://openai.com/index/securing-research-infrastructure-for-advanced-ai>

⁴⁴<https://cloudsecurityall.org/star/registry/openai/services/openai-api-chatgpt-enterprise-teams-dalle>

⁴⁵<https://openai.com/policies/supplier-security-measures/>

Business kliendil on võimalik seadistada⁴⁶:

- mitmikautentimine (MFA),
- rollipõhine õiguste jagamine, rollid on: Member, Admin, Owner,
- reguleerida kasutaja juurdepääsu kolmanda osapoole GPTdele,
- ainulogimisega pöördumine (SAML SSO).

Enterprise kliendil on võimalik⁴⁷:

- kõik, mis Business kliendilgi, lisaks oma jõudeolekus ja vaikumisi krüpteerimisega kaitstud sisu enda hallatavate võtmetega teistkordselt krüpteerida (ümbriskrüpteerimine, (envelope data encryption))⁴⁸,
- määrata kasutajakontodele ressursse ja õigusi automaatselt (hoole, provisioning) ning ka vabastada (tagandus, deprovisioning) (SCIM),
- luua uusi rolle, neid gruppideks organiseerida ja seada õiguseid erinevate tegevuste sooritamiseks (connectors, shared projects, GPTs, web search).

SOC 3 teise tüübi raporti⁴⁹ järgi eksisteerib hoolimata tõhusate turvameetmete rakendamisest võimalus inimliku eksimuse tekkeks ja turvameetmetest möödapääsemiseks. Vajalik on kliendipoolsete meetmete rakendamine: juurdepääsukontroll, probleemide raporteerimine OpenAI-le. Samuti tuleb kliendil jälgida, kas ta on oma andmete kasutamise mudelite treenimiseks lubanud või keelanud ning et andmete kustutamine

oleks seadistatud kliendi vastava poliitika kohaselt.

RiskRubic.ai⁵⁰ AI-mudelite riskihinnangu järgi ei ole GPT-4 mudelid läbipaistvad, küll aga on saanud kõrged hinnangud ülejäänud viies kategoorias. GPT-5 mudelid on saanud kõrged hinnangud kõigis kuues kategoorias.

AI-spetsiifilised nõrkused: OpenAI Assistant API võimaldab väärkasutust⁵¹: kasutaja arvutis olev kahjurvara kasutab Assistant API liidest juhtkanalile (command-and-control, C2) kus API kaudu saavad krüpteeritud käsud ja andmed liikuda pahatahtlikul eesmärgil. OpenAI ei tõlgenda seda oma teenuse nõrkusena, vaid väärkasutusena.

OpenAI deklareerib, et nii teenustaja enda seatud reeglite kui ka EL- i tehisintellekti määrusest tulenevate nõuete täitmise tagamiseks on juurutatud meetmeid, mis aitavad teenuse väärtarvitusi tuvastada ja tõkestada. Meetmed hõlmavad nii automatiseeritud protsesse (klassifikaatoreid, blokeerimisnimekirju, arutlusmudelid, räsi vastavuse kontrolli jm) kui ka inimeste tehtavaid ülevaatusi. Ühtlasi rõhutab teenustaja eeldust ja ootust, et kliendid kasutavad teenust vastutustundlikult^{52 53}.

Reegleid rikkuva kasutusviisi tuvastamisel võetakse kasutajad vastutusele, sealjuures võidaks väärtarvitajalt ära võtta juurdepääs teenusele⁵⁴. Konkreetse mudeli treenimise viisi, ohutushinnangut (safety evaluations) ja riskide leevendamise meetmeid vaata vastava mudeli kaardilt (system card)⁵⁵.

Soovitus: kontrollida, et mudelite treenimine andmete põhjal poleks lubatud

⁴⁶<https://openai.com/business-data/>

⁴⁷<https://chatgpt.com/business/enterprise>

⁴⁸https://help.openai.com/en/collections/2000094_1-enterprise-key-management-ekm

⁴⁹<https://trust.openai.com/?itemUid=27a3eac6-90c8-402d-ald8-817e02eb07f0&source=title>

⁵⁰<https://riskrubic.ai/>

⁵¹<https://www.bleepingcomputer.com/news/security/microsoft-sesameop-malware-abuses-openai-assistants-api-in-attacks/>

⁵²<https://openai.com/transparency-and-content-moderation/>

⁵³<https://help.openai.com/en/articles/10658393-complying-with-the-eu-ai-acts-prohibited-practices-requirements>

⁵⁴<https://openai.com/en-GB/policies/usage-policies/>

⁵⁵<https://trust.openai.com/?itemUid=092e78c8-b5c8-4428-ac96-c357c088ef66&source=click>

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 pakujale/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 kvaliteedimõdikuid 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	<p>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.</p> <p>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, reaajas jälgimine ja võimalus sulgeda, muuta või lasta inimesel sekkuda süsteemidesse, mis erinevad kavandatud või oodatud funktsionaalsusest.</p>
	<p>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.</p> <p>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.</p>
	<p>Andmete kustutamises ei saa veenduda, kuna konto üleminekul on võimalik kontrol olev andmestik kolmandale isikule edasi anda (nt juhile). Ei saa kontrollida, kas andmed on kustutatud.</p> <p>Sätendada asutusesisene protseduur andmete kustutamise osas.</p>
	<p>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).</p> <p>Rakendada asutusesiseseid protsesse ja poliitikat, 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.</p>

Kokkuvõte

OpenAI on rakendanud infoturbe ja andmekaitse alaseid meetmeid, millega saab lugeda ChatGPT teenus usaldusväärseks. ChatGPT andmete majutamise võimalus on nii Euroopa Liidus kui ka mujal maailmas, konkreetne valik sõltub valitud teenusest.

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

Vajalik on rakendada täiendavaid meetmeid paralleelselt ChatGPT kasutamisega, mh koolitada kasutajaid, veenduda, et toodet ei kasutataks keelatud viisil, arendada alternatiivseid töömeetodeid, kontrollida ChatGPT 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 ChatGPT sobiv kasutamiseks. Arvesse tuleks võtta AI kasutamisega ja pilvtoodetega seonduvaid riske ning OpenAI poolt rakendatud meetmeid turvalisuse tagamiseks.

