Atlassian AI

Kirjeldus

Käesolev usaldusväärsuse hinnang on Atlassiani usaldusväärsuse hinnangu lisa ja keskendub Atlassian AI pilvtöötlusteenuse riskide kirjeldamisele ning ei kohaldu Atlassiani 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].

Atlassian AI on Atlassiani toode, mis on mõeldud kliendi toetamiseks ja aitamiseks. Atlassian AI on sisuliselt mitte teenus, vaid geneeriline raamistik koos funktsioonistikuga, mida on võimalik integreerida a) peaaegu igasse Atlassiani tootesse, b) kliendi peaaegu mistahes töötlusjuhtu Atlassiani toodete piires.

Atlassian Intelligence on tehisintellekti funktsioonistik, mis on integreeritud kõigisse Atlassiani toodetesse. Atlassian Intelligence kasutab nii ettevõttesiseselt kui ka OpenAI arendatud tehisintellektimudeleid Atlassiani toodete rikastamiseks.

Atlassian asutati 2001. aastal kahe kolledzikaaslase Mike Cannon-Brookes ja Scott Farquhar koostöös. Esimese Atlassiani tootena jõudis turule Jira 2002. aastal ning seejärel Confluence 2003. aastal.

Jira ja Confluence esimesed pilveversioonid nägid ilma 2011. aastal. Atlassian Intelligence tuli välja ning sai avalikult kättesaadavaks 2023. aasta lõpus. Atlassian on pühendunud tehisintellekti vastutustundlikule arendamisele ning on avaldanud oma vastutustundliku tehnoloogia põhimõtted[2]. 2024. a septembris liitus Atlassian Euroopa AI (tehisintellekti) paktiga[3].

Atlassianil on hetkel käsil turunduslik restruktureerimine, mille käigus paljud (kuid mitte kõik) seni Atlassian Intelligence nime all reklaamitud teenused ja tegutsemissuunad nimetatakse ümber Rovo AI-ks. Muudatused olid usaldusvääruse hinnangu koostamise hetkel käimas, mistõttu pole kindel, millist nime mingi konkreetne teenus kannab näiteks järgmisel kuul.

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

[1]

[2] https://www.atlassian.com/trust/responsible-tech-principles

[3] https://www.atlassian.com/trust/compliance/resources/eu-ai-act

Teenuse võimalused

Atlassian Intelligence ei ole iseseisev toode ega teenus ning seetõttu ei ole klassifitseeritav pilvteenusena ISO/IEC 22123-1:2023 standardi kohaselt. See on turunduslik määratlus, tehisintellektil põhinev funktsioonide kogum, mis on integreeritud Atlassiani toodetesse ning on automaatselt kättesaadav kõigile Standard, Premium ja Enterprise pakettide tellijatele. Funktsioonistik on vaikimisi sisse lülitatud, võib erineda toodete lõikes ning on väga kiires muutuses. Organisatsiooni administraatorid saavad selle halduskeskuses toodete kaupa välja ja sisse lülitada; Atlassian Intelligence funktsioonide väljalülitamine ei mõjuta teenuse väärtuspakkumist. Atlassian Intelligence võtab arvesse tootesiseseid pääsuõigusi ning lubab kasutajal näha ja muuta ainult seda sisu, milleks tal on luba/õigus.

Atlassian Intelligence kasutab mitmesuguseid avatud lähtekoodiga ja ettevõttesiseseid suuri keelemudeleid (LLM), sealhulgas Llama, Phi ja Mixtrali seeria mudeleid, ning lisaks ka kolmandate osapoolte suuri keelemudeleid OpenAI GPT-seeriast, Anthropic Claude seeriast ja Google Gemini seeriast. Optimaalse mudelite kombinatsiooni leidmiseks kasutatakse dünaamilist valikut (dynamic routing), mis tagab iga kasutusstsenaariumi puhul parima kasutuskogemuse ja täpsuse.

Atlassian Intelligence abiga saab:

- luua sisu Confluence'is, Jira's, Jira Service Management'is, Bitbucket'is ja Trello's, nt saab kasutada ajurünnaku (Brainstorming) funktsiooni, mis aitab genereerida ideid;
- redigeerida sisu, nt muuta suhtluse tooni, teha kokkuvõtteid, parandada vigu jne;
- kokku võtta sisu Jira Service Management'is, Jira's ja Confluence'is;
- seadistada automaatprotsesse Confluence'is, Jira's ja Jira Service Management'is;
- otsida spetsiifilist teavet Jira's, kasutades keerukate päringute tegemisel loomulikku keelt;
- luua SQL päringuid Atlassian Analytics'is;
- kasutada päringu tuubi sõnastamist Jira Service Management kliendiportaalis.

Atlassian Intelligence on aktiivses arenduses ning seetõttu lisandub pidevalt uusi kasutusvõimalusi.

Atlassian Intelligence'i kasutamisel edastatakse andmed vastuse genereerimiseks kolmandate osapoolte LLM teenustajatele (nt OpenAI). Andmete edastamisel järgitakse Atlassian'i turvatavasid ning saadetakse iga andmepäring eraldi SSL-krüpteeritud teenuse kaudu. Kasutatavate suurte keelemudelite teenustajad ei talleta kliendi sisendeid ega väljundeid ega rakenda neid oma teenuste parendamiseks.

Atlassian Intelligence käideldavusaspektid on kaetud üldise Atlassiani teenustasemelepinguga, milles on märgitud tasemekohustumus Premium tellimuse puhul 99.9% ning Enterprise tellimusel 99.95%[4].

EL tehisintellekti määruse kohane riskitase

Atlassian AI riskitase sõltub konkreetsest kasutusjuhust. NB! Atlassian rõhutab, et 828 ettevõttena annab oma klientidele selgelt teada, et nende tooteid ei peaks ega tohi kasutada teatud eesmärkidel. Selleks on kasutamispoliitika (Acceptable use

[4] https://www.atlassian.com/legal/sla#service-credits

policy) uues, tehisintellekti käsitlevas jaotises selgitatud, et Atlassiani tehisintellektil põhinevaid tooteid ei tohi kasutada asjaoludel, mida peetaks asjakohaste seaduste alusel või teadaolevate tehisintellektispetsiifiliste riskide tõttu kõrge riskiga olukordadeks[5].

Soovitus: kontrollida, millised on kõrge riskiga olukorrad, milleks toodet kasutada ei tohi

Kasutusjuhud

Atlassian AI funktsiooniga on hõlmatud järgnevad toimingud:

- sisu loomine Confluence'is, Jira's, Jira Service Management'is, Bitbucket'is ja Trello's;
- sisu redigeerimine;
- sisu kokkuvõtmine Jira Service Management'is, Jira's ja Confluence'is;
- automaatprotsesside seadistamine Confluence'is, Jira's ja Jira Service Management'is;
- loomuliku keele toega otsing Jira's;
- SQL päringute loomine Atlassian Analytics'is;
- päringu tüübi sõnastamine Jira Service Management kliendiportaalis.

Rahaline mõju

Atlassian Intelligence kaasneb pakettidega Standard, Premium ja Enterprise automaatselt ning selle funktsioonistiku aktiveerimise eest ei võeta eraldi tasu[6].

Atlassiani toodetele kehtiva hinnakirjaga saab tutvuda soovitud toote lehel, nt Jira, Confluence jt.

Soovitus: tutvuda hinnakirjaga ning veenduda, et ei kaasneks täiendavaid kulusid

EL/NATO liikmesriigis hoitavad andmed

Atlassian kasutab oma pilvrakenduste ning andmete majutamiseks (jms) Amazon Web Services (AWS) kõrgkäideldavaid andmekeskusi üle maailma[7]. Standard, Premium ja Enterprise paketi tellijatel on võimalus valida geograafiline regioon andmete talletamiseks. Andmete asukoha valik on saadaval Jira, Confluence, Jira Service Management ja Jira Product Discovery toodete puhul[8].

GDPR-i kohaselt võib andmeid edastada väljapoole Euroopa Liitu kui on rakendatud asjakohased kaitsemeetmed (artikkel 46[9]).

Andmete asukoht sõltub seega teenuse infrastruktuurist ja Atlassiani serverite asukohtadest. Täpsemalt on kirjeldatud Atlassiani usaldusväärsuse hinnangus.

Soovitus: kontrollida, kus teenusepakkuja andmeid majutab

[5] https://dam-cdn.atl.orangelogic.com/AssetLink/214k4h05d588o68kx6014730p3abx6s4.pdf
[6] https://support.atlassian.com/organization-administration/docs/what-is-atlassian-intelligence/
[7] https://www.atlassian.com/trust/reliability/cloud-architecture-and-operational-practices#atlassian-cloud-hosting-architecture
[8] https://www.atlassian.com/software/data-residency
[9] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&qid=1689851996164

Teenusest lahkumise ja andmete ekspordi võimalus

Atlassian võimaldab eksportida pilvrakenduste ning kasutajate andmeid, täpsemad tingimused on ära toodud vastaval lehel. Klientidel on võimalus täielikult eemaldada kõik enda andmed loetletud Atlassiani pilvteenustest (Confluence, Jira (sh Jira Software, Jira Service Management, Jira Work Management, Jira Product Discovery) ning Opsgenie), mida kasutatakse Standard, Premium ja Enterprise tellimusega. Andmete eemaldamise täpsema protseduuriga saab tutvuda Atlassiani toe lehel.

Teenuse taastamiseks tehtavaid varukoopiaid ei kasutata kliendi enda sooritatud andmemuutmise või kustutamise tagasipööramiseks andmekao vältimiseks tuleb kliendil varundus korraldada endal[10].

Andmeid töödeldakse ja säilitatakse vastavalt teenuse kasutamisele ning vajadusele. Andmekao vältimiseks peaks andmete omanik hindama Atlassian AI pilvteenuses olevat andmete koosseisu ning nende ajaloolist väärtust, et hinnata, kas andmete eksportimine on vajalik ja otstarbekas.

Soovitus: kontrollida andmete kustutamise, varundamise ning eksportimisevõimalusi

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

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid[11].

Kuigi teenustaja kodulehel on olemas ISO/IEC 27001:2022 sertifitseerituse märgis, ei õnnestunud leida seda kinnitavat kehtivat sertifikaati, mis oleks avalikult kättesaadav. Atlassianil siiski oli ISO/IEC 27001:2013 sertifikaat, mis aegus 2025. a jaanuaris.

Atlassian on Cloud Security Alliance'i (CSA) korporatiivliige ning on ühtlasi ka CSA usaldusväärsete pilveteenuse pakkujate nimekirjas. Õigustatud isikud saavad tutvuda SOC2 raportite ja teiste asjakohaste sertifikaatidega Atlassian'i usalduskeskuses[12].

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

[10] https://www.atlassian.com/trust/reliability/cloud-architecture-and-operational-practices#cloud-infrastructure

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

[12] https://www.atlassian.com/trust/compliance/resources

riskipõhisest lähenemisviisist ehk AI süsteeme tuleb analüüsida ja klassifitseerida vastavalt sellele, millist ohtu need kasutajatele kujutavad. Samas ei tohi ära unustada ka kehtivat õigusraamistikku[13].

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)[14]. AI määrus kirjeldab ka, millised on riskitasemed AI süsteemide osas ning reguleerib ka AI süsteemide kasutamist ja määratleb rikkumisest teavitamise võimalused (nt järelevalveasutuse).

Kui AI süsteem või seda opereeriv isik kuulub määrus(t)e kohaldamisalasse, tuleb hinnata, millised konkreetsed nõuded määrus(te)st tulenevad GDPR-i kohaselt on oluline hinnata, kas kvalifitseerutakse näiteks isikuandmete vastutavaks või volitatud töötlejaks, AI määruse puhul aga näiteks AI-süsteemi teenustajaks ("provider") või juurutajaks ("deployer"). Määruste kohaseid rolle on veelgi ja ka need on mõistlik üle vaadata. Konkreetsete nõuete tuvastamiseks on vaja teada ka seda, mis on andmetöötluse ja AI kasutamise eesmärk, millised andmetöötlusprotsessid süsteemis toimuvad, millised andmed ja kelle vahel liiguvad ning millist AI-süsteemi või komponenti (sh selle riskitase) süsteemis kasutatakse[15].

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[16].

Täpsemalt on kirjeldatud Atlassiani usaldusväärsuse hinnangus.

Soovitus: kontrollida olemasolevate sertifikaatide kehtivust ja vastavust KüTSile

Andmekaitse meetmete rakendamine

Atlassian AI kasutamine on reguleeritud kliendilepinguga (Customer Agreement, kehtivus alates 7.oktoober 2025)[17] ning selles viidatud lisadega. Lisade hulka kuulub andmetöötlusleping (Data Processing Agreement)[18]. Atlassiani veebilehel on kinnitatud, et eeltoodud dokumendid hõlmavad Atlassian Intelligence and Ravo funktsionaalsuseid [8].[19] Atlassiani privaatsuspoliitika (Privacy Policy) reguleerib olukordi, kus vastutavaks töötlejaks on Atlassian[20].

Privaatsuspoliitikas ja kliendilepingus on viidatud, et olukorras, kus Atlassian tegutseb volitatud töötlejana kliendile teenust pakkudes, kohaldub andmetöötlusleping. Lisaks on Atlassianil üldise AI tingimused (Atlassian AI Terms)[21].

[13] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[14] https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf
[15] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[16] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[17] https://www.atlassian.com/legal/atlassian-customer-agreement#intro
[18] https://www.atlassian.com/legal/data-processing-addendum#scope-and-term
[19] https://www.atlassian.com/trust/atlassian-intelligence
[20] https://www.atlassian.com/legal/privacy-policy#privacy-policy-overview
[21] https://www.atlassian.com/legal/ai-terms#intro

Andmetöötluslepingu kohaselt teavitab Atlassian klienti turvaintsidendist 72 tunni jooksul alates sellest teada saamisest.

Kui seadus ei nõua teisiti, siis kliendi ja Atlassiani vahelise lepingu lõppemisel kustutab Atlassian kõik isikuandmed, kooskõlas Atlassiani varundus- või andmete säilitamise poliitikatega (standard backup or record retention policies).

Atlassian edastab isikuandmeid kolmandatesse riikidesse. Atlassian ei too välja töödeldavate isikuandmete täpset loetelu, vaid selgitab, et töötleb kliendi isikuandmeid, mille sisu määratleb ja kontrollib ainult klient oma kasutajatega[22].

Atlassian kasutab alltöötlejaid. Alltöötlejate nimekiri on leitav Atlassiani kodulehel.

Kliendileping sisaldab üldist konfidentsiaalsusklauslit. Kliendilepingu järgi peab klient tagama, et tal on kõik vajalikud õigused ja nõusolekud, et kliendiandmeid (Customer Data) Atlassiani teenustes kasutada[23].

Atlassiani AI tingimused keelavad Atlassianil kasutada kliendi poolt AI funktsioonidesse sisestatud või vastuseks saadud andmeid oma mudelite treenimiseks või täiendamiseks[24].

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, millistesse kolmandatesse riikidesse Atlassian andmeid edastab

Erinõuded

Nõuded teenustajale: Nõuded teenustajale sõltuvad tuvastatud riskitasemest.

Nõuded kasutusele võtjale: Nõuded kasutusele võtjale sõltuvad tuvastatud riskitasemest.

Atlassian ei luba kasutada enda tehisintellektitooteid ja -funktsioone selleks, et[25]:

- pakkuda või otsida nõu, mida tavaliselt annavad kvalifitseeritud või litsentseeritud spetsialistid, sh õigus-, meditsiini/tervise-, finantsvaldkonnas, või mistahes muud professionaalset nõustamist;
- teha automaatotsuseid, mis võivad põhjustada õiguslikke vms tagajärgi, sh valdkondades, mis võivad mõjutada üksikisiku õigusi, ohutust, tervist või heaolu (nt rahanduse, laenu, kindlustuse, tööhõive, eluaseme, hariduse, esmatähtsate teenuste, õiguse või õiguskaitse, rände, kriitilise taristu haldamise, kohtumenetluse või sotsiaalhindamise valdkondades);
- võtta osa tegevustest, mis on kasutusviisile ja loodud väljundile kohalduvate asjakohaste riigiseaduste alusel klassifitseeritud keelatud või kõrge riskiga kasutusviisiks, sh näiteks

-teha järeldusi isiku emotsioonide kohta töö- ja õppekeskkonnas;

-kategoriseerida isikuid nende biomeetriliste andmete abil, et tuletada tundlikke atribuute (nt rass või poliitilised vaated);

-hinnata või klassifitseerida isikuid nende sotsiaalse käitumise või isikuomaduste

[22] https://www.atlassian.com/legal/data-processing-addendum#scope-and-term

[23] https://www.atlassian.com/legal/atlassian-customer-agreement#intro

[24] https://www.atlassian.com/legal/ai-terms#intro

[25] https://www.atlassian.com/legal/acceptable-use policy#ai-offerings

põhjal viisil, mis põhjustab kahjuliku või ebasoodsa kohtlemise;

- tegeleda poliitiliste kampaaniate või lobitööga, sh luua kampaaniamaterjale poliitilise protsessi mõjutamiseks või takistamaks osalemist protsessides;
- panna inimesi uskuma, et nad suhtlevad inimesega juhul kui see nii ei ole.

Rikkumiseks loetakse, kui Atlassiani tehisintellektitoodete või funktsioonide abil:

- püütakse mööda hiilida Atlassiani teenuste kaitsmiseks mõeldud tehnilistest või turvameetmetest või neid eirata, nt selliste tehnikate abil nagu prompt injecting ja jailbreaking, või tahtlikult suunata teenuseid tegutsema viisil, mis rikub ülalmainitud reegleid;
- esinetakse teise isiku või organisatsioonina ilma nende vastava nõusoleku või loata, või ilma vastava seadusliku aluseta;
- tegeletakse võlts- või väärteabe ning võltsitud veebiarvustuste loomise või levitamisega, plagiaadi või akadeemilise petturlusega;
- peetakse erootilist, romantilist või seksuaalse alatooniga vestlust.

Soovitus: kontrollida, et toodet ei kasutataks keelatud viisidel

Turvameetmete rakendamine

Turvameetmete ülevaate allikaks on Atlassiani arhitektuuri ja talitluspraktikate kirjeldus[26]. Füüsilise turvalisuse osas tugineb Atlassian AWS andmekeskuste turvameetmetele.

Asurid on teineteisest eraldatud loogiliselt. Tagamaks, et kõik teenustele tehtavad päringud on seotud kindla asuriga, kasutatakse asuri kontekstiteenust (tenant context service, TCS). Juurdepääs Jira ja Confluence andmetele toimub ainult siis, kui see kontekst on olemas. Teenuste autentimine ja loastamine toimuvad ASAP-protokolli kaudu koos lubatud teenuste nimekirjaga. Väljuvat liiklust ja juurdepääsu teenustele piiravad spetsiaalsed vaheserverid, mis kompromiteeritud teenuse korral takistavad ründaja külgsuunalist edasiliikumist ning välistavad rakenduse koodinõrkuste toime turvamehhanismidele. Sissetungituvastus hosti tasemel ja konteineripiirid lisavad täiendava kaitsekihi.

Andmetele juurdepääs on piiratud minimaalõiguste põhimõttel. Teenused kasutavad JWT (JSON web token) pääsulubasid identiteedi kontrollimiseks ja kindlustamaks, et andmetele pääseb juurde ainult volitatud teenus. Lisaks on asuri kontekstteenus tugevalt replitseeritud, mis võimaldab anomaaliad tuvastada kiiresti. Atlassian tegeleb regulaarselt ka turvariskide ennetava avastamise ja neile reageerimisega.

Liikvel andmed on krüpteeritud TLS 1.2+ protokollidega. Pilvteenustesse Jira Software Cloud, Jira Service Management Cloud, Jira, Bitbucket Cloud, Confluence Cloud, Statuspage, Opsgenie ja Trello salvestatud kliendi jõudeolekus andmed {sh manused) on krüpteeritud AES-256 algoritmiga. Atlassianil on olemas krüpteerimispoliitika, mis sätestab põhimõtted krüptograafia rakendamiseks isikuandmete kaitsmisel vastavalt andmete liigitusele.

[26] https://www.atlassian.com/trust/reliability/cloud-architecture-and-operational-practices#cloud-infrastructure

Võtmehalduseks kasutatakse AWS võtmehaldusteenust {KMS). Osade teenuste[27] puhul on võimalik kasutada isegenereeritud võtmeid (bring-your-own-key, BYOK)[28]. Toetamata rakenduste puhul peavad kliendid omi riske hindama ise enne nende teenuste kasutamist.

lgast Amazon RDS (Relational database service) isendist tehakse krüpteeritud {AES-256) varukoopia korra päevas. Varukoopiad dubleeritakse sama regiooni andmekeskustesse, neid hoitakse 30 päeva ja neid testitakse regulaarselt.

Atlassian on liitunud EU AI Pactiga ning on võtnud selle raames viis kohustust[29].

- tehisintellekti juhtimise organisatsioonilise strateegia vastuvõtmine;
- kõrge riskiga AI käsitlemine toodetes ja protsessides;
- •töötajate koolitamine tehisintellekti ja selle mõju osas;
- läbipaistvus Atlassiani tehisintellekti kasutajatele;
- AI süsteemide kavandamine viisil, et kasutaja oleks teadlik AI kasutamisest.

Nende kohustuste täitmiseks rakendab Atlassian järgnevaid meetmeid:

- AI juhtimise strateegia rakendamine ettevõttesiseselt;
- Vastutustundliku tehnoloogia ülevaated (Responsible Technology Reviews RTR} AI toodete ja kasutusjuhtude hindamiseks;
- AI lüüs (AI Gateway}, mis kontrollib juurdepääsu alusmudelitele prototüüpide loomise, arendamise jms eesmärgil ning see lüüs rakendub nii ettevõttesiseste kui ka -väliste kasutusjuhtude puhul. Heakskiidu (juurdepääsu} saamiseks on vaja läbida RTR-protsess, mis tagab, et kavandatud kasutusotstarvet on põhjalikult uuritud juba enne heakskiidu andmist;
- kasutamispoliitika (AUP} uuendamine, mis keelab suure mõjuga otsuste tegemise, professionaalsete nõuannete andmise ja tegevused, mida peetakse kõrge riskiga tegevusteks;
- tehnilised kaitsemeetmed, mh tootesised filtrid, mis takistavad keelatud päringuid ja tuletavad kasutajatele piiranguid meelde;
- läbipaistvuse tagamine, kavandades tooteid selliselt, et kasutajal on võimalik ara tunda AI olemasolu.

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.

[27] https://support.atlassian.com/security-and-access-policies/docs/data-managed-with-byok-encryption/
[28] https://www.atlassian.com/trust/privacy/byok
[29] https://dam-cdn.atl.orangelogic.com/Assetlink/214k4h05d588o68kx6014730p3abx6s4.pdf

AI-ga seotud riskid	**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.**
	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**

AI-ga seotud riskid	
	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

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

Atlassian AI pakub klientidele võimalusi, kuidas muuta kasutajate töö produktiivsemaks ja kulutõhusamaks. Atlassiani klientidel on võimalus seadistada Atlassian AI 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 Atlassian AI teenuse katkematust tööst.

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