xLaw

Kirjeldus

Käesolev usaldusväärsuse hinnang keskendub xLaw pilvtöötlusteenuse (edaspidi xLaw) riskide kirjeldamisele ning ei kohaldu xLaw 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.

Extendlaw (edaspidi xLaw) OÜ peakontor asub Tallinnas. xLaw on juristidele loodud teadmushaldussüsteem ja digitaalne abiline, mis kiirendab ja optimeerib tööprotsesse ning aitab tehisintellekti abil andmeid süstematiseerida. xLaw on 2016. aastal asutatud ettevõte, mille omanike hulgas on Evert Nõlv (80% osalusega} ning Monika Nõlv (20% osalusega}. xLaw rakenduse esimene versioon on loodud aprillis 2015.

xLaw on kasutusel kõikides Eesti kohtutes ning enam kui 70 advokaadibüroos. Chrome'i veebipoes on kasutajad hinnanud rakenduse 5 punktiga viiest[1].

xLaw on pilvelttarkvara (Saas)[2]. xLaw rakendus ühildub juristide peamiste töökeskkondadega, nagu riigiteataja.ee (xLaw RT), riigikohus.ee (xLaw RK), eur-lex. europa.eu (xLaw EU), curia.europa.eu ning MS Word (xLaw Word). Lisaks viiele põhimoodulile, sh õigusteabe otsinguportaaliga legal.ee ühilduv moodul xLaw Legal, on rakenduses alates 2025. aastast võimalik kasutada tehisintellektil põhinevat abilist (AI Assistant), mis on sisult otsingumootor. Samuti saab kasutada tehisintellekti genereeritud kokkuvõtte funktsiooni (AI kokkuvõte) ning xLaw Outlook moodulit[3] e- kirjade põhjade loomiseks, haldamiseks ja taaskasutamiseks. xLaw'l on mobiiliäpp mobiiltelefonidele ja tahvelarvutitele (iOS, Android) - Eestis kehtivate seaduste sisu on kasutamiseks tasuta (sh otsing), rakenduse allalaadimisel on ühekordne tasu (2025. aastal 9.99 EUR). Mobiiliäpi funktsioonistik on piiratud, näiteks saab kasutaja näha lisatud kommentaare ja linke.

Kõik xLaw moodulid on omavahel seotud ning kasutaja kommentaarid on ristkasutatavad sõltuvalt mooduli funktsioonidest. Kommentaare näevad kõik ühte gruppi kuuluvad kasutajad.

[1] https://chromewebstore.google.com/detail/xlaw/kfngooidkiiljlbpaafgcfjddkgnhjkl/reviews

[2] https://digikogu.taltech.ee/et/itern/52f8b383-9ff0-449f-9000-e01530de05b0

[3] https://extendlaw.com/uudised/xlaw-outlook-uus-tooriist-e-kirjade-haldamiseks

xLaw Word'il on liidestus Eesti äriregistriga, et vajalik teave oleks koheselt kättesaadav ilma käsitsi ümberkopeerimiseta või eraldi veebilehe külastamiseta[4].
Sisselogimine on võimalik e-mailiga või kolmandate poolte (gatekeepers) konto kaudu:

- Google (gmail.com);
- Facebook;
- Microsoft.

xLaw rakendus on allalaetav pistikprogrammina veebilehitsejatele: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari.

Selleks, et saaks kasutada kõiki xLaw mooduleid, tuleb sisse logida sama kasutajanime ja - parooliga kolmes kohas:

- xLaw pluginas (Chrome/Firefox/Edge/Safari) - et saaks kasutada xlaw RT, xLaw EU, xLaw RK;
- xlaw Word'is (Microsoft Word add-in) - et saaks kasutada xLaw Word;
- xLaw Legal'is (veebilehel legal.ee) - et saaks kasutada xLaw Legal.

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

EL tehisintellekti määruse kohane riskitase

xLaw on kõrge riskiga süsteem AI määruse kohaselt, kuna AI funktsioone kasutatakse õigusemõistmise valdkonnas (AI Act Annex III). Tehisintellekti poolt loodud sisu võib potentsiaalselt mõjutada juristide ja õigusteadlaste otsuste tegemist ning seeläbi füüsiliste isikute õigusi. Võimalik, et kohaldub mõni AI määruse artikli 6 lõikes 3 välja toodud erand, kuid see vajab täiendavat analüüsi ning suhtlust teenustajaga. Samuti võib riskitaseme määratlust muuta tulevane (kohtu) praktika.

xLaw puhul ei saa välistada, et see osutub kõrge riskitasemega AI-süsteemiks. Kui nii, siis tuleks seda kasutavatel organisatsioonidel läbi viia andmekaitsealane mõjuhindamine. Puudub täpne teave integratsiooni ulatusest avaliku pilvega, seda eriti Wordi dokumentide osas, mis õigusvaldkonnas paratamatult sisaldavad isikuandmeid.

Soovitus: Teenustaja märgistab selgelt eristaval viisil tehisintellekti poolt loodud sisu ning hoiatab, et see võib sisaldada vigu.

Teenuse puudused

xLaw pilvteenuseid majutatakse väljaspool Eesti territooriumi ning vajavad üldiselt toimimiseks püsivat Interneti ühendust. Ühenduseta xLaw pilve pikaajalise katkestuse korral on vajalik kasutada alternatiivseid rakendusi.

Eesti riigiasutuste jaoks on oluline teabevahetuse korraldamine ka olukordades, kus välisühendused halvatakse kas pahatahtliku ründe tõttu või on sunnitud riik ennetava meetmena ise ühendused katkestama[5].

XLaw annab endast parima, et rakenduse funktsionaalsus kasvatamiseks ning tagamaks, et tarkvara töötaks ilma tõrgeteta. Sellegipoolest ei saa xLaw garanteerida, et rakenduse toimimises ei teki tõrkeid ega anna muid garantiisid rakenduse kvaliteedi ega funktsionaalsuse osas. xLaw ei vastuta kahju eest, mis tekib sellest, et veebileht või rakenduse kasutus on tehnilistel või muudel põhjustel võimatu"[6].

Avalikult kättesaadavates materjalides ei ole xLaw avaldanud spetsiifilisi juhiseid AI ohutuks kasutamiseks oma teenustes. Ei privaatsuspoliitika ega kasutustingimused ei anna AI - spetsiifilisi ohutusjuhiseid.

[4] https://digikogu.taltech.ee/et/itern/52f8b383-9ff0-449f-9000-e01530de05b0

[5] https://www.aki.ee/sites/default/files/ringkirjad/andmetootlusest_avalikes_pilveteenustes_0.pdf

[6] https://xlaw.eu/tos.html

AI süsteemi andmekaitsealastele nõuete tagamiseks peab võtma arvesse IKÜMi artikli 5 lõikes 1 kehtestatud isikuandmete töötlemise põhimõtteid, mille täitmise eest vastutab ja peab olema võimeline nõuete täitmist tõendama vastutav töötleja (IKÜM artikkel 5(2)).

USA-s tegutsevatele isikutele ja asutustele ja/või USA-s asuvatesse andmekeskustesse isikuandmete edastamine ei ole üldjuhul lubatud, sest Euroopa Liidu ja Ühendriikide vahel ei ole alates 2020. aasta juulikuust[7], mil Euroopa Kohus tunnistas kehtetuks *Privacy Shield'i* nimelise andmekaitseraamistiku, toimivat andmekaitsealast koostööd ning andmete edastust. Sellega seoses ei ole andmesubjektidele USA-s toimuva andmetöötluse osas tagatud samaväärsed õigused (ei pruugi olla tagatud turvameetmed, võidakse teostada andmekorjet või edastada andmeid kolmandatele isikutele, nt järelevalveasutused, vt ka *CLOUD Act*[8]), nagu kehtivad Euroopa Liidus toimuva andmetöötluse suhtes. Varasemad lepped EU ja USA vahel on korduvalt õigustühiseks tunnistatud. Töö uue vastava andmekaitseraamistiku loomise nimel käib siiski aktiivselt ja selle heakskiitmist võib prognoosida 2024. aasta jooksul. 2023 aastal vastu võetud *Data Privacy Frameworki* kohaldami se osas töö käib ja selle funktsionaalsust hinnatakse perioodiliselt (kontrollitakse, kas kõik asjakohased meetmed on rakendatud ning toimivad praktikas, et kaitsta isikuandmete edastamist EU-USA vahel).[9]

Soovitus: kontrollida, milline on pilvandmetöötluse katkemise mõju protsessidele

Töötlusjuhud

- xLaw Legal otsinguportaali kasutaja genereerib AI vahendusel kokkuvõtteid seadusesätte tõlgendusest.
- xLaw Legal otsinguportaali kasutaja esitab AI Assistendile täpsustavaid küsimusi leitud otsingutulemuste kohta.
- AI Assistant genereerib vastuse 10 kõige uuema lahendi põhjal tekkinud küsimustele.

Sisu uuendamise vajadust kontrollib ja sisu uuendab veebirobot korra päevas[10]. Kui Riigi Teatajas muudetakse lahendi sisu (eemaldatakse isikuandmeid}, siis uueneb ka antud lahend xLaw süsteemides.

Rahaline mõju

xLaw valikus on kolm standardpaketti:

- Professionaal, mis sisaldab kõiki funktsioone (85 EUR + KM kasutaja/kuus 2025. aastal};
- Grupp, mis sisaldab kõiki funktsioone ning on mõeldud vähemalt neljale kasutajale;
- Tudeng, mis on piiratud funktsionaalsusega ning mõeldud õigustudengitele (tasuta juurdepääs}; lisaks sellele on tudengitel võimalik tellida ligipaas täisversioonile 70% -lise allahindlusega[11].

[7]EKo 16.07.2020, C-311/18 – Data Protection Commissioner vs Facebook Ireland Ltd, Maximillian Schrems

[8] https://en.wikipedia.org/wiki/CLOUD_Act

[9]https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_et

[10]https://digikogu.taltech.ee/et/itern/52f8b383-9ff0-449f-9000-e01530de05b0

[11]https://extendlaw.com/xlaw/xlaw-tudengipakett

2025. aastal on xLaw valikus neli paketti valdkonnaspetsialistidele[12]:

- Riigihangete pakett - hankespetsialistile ja riigihangete vaidlustele spetsialiseerunud juristidele;
- KOV pakett kohaliku omavalitsuse töötajale;
- Raamatupidaja pakett raamatupidajale;
- Tööõiguse pakett personalispetsialistile ja tööõigusele spetsialiseerunud juristidele.

Täpsema hinnakirjaga on võimalik tutvuda xLaw kodulehel[13].

Rakenduse kasutustingimustes on märgitud, et kasutustingimuste jõustumise hetkel pakutakse teatud funktsioone tasuta, kuid ei tagata nende tasuta kättesaamise jätkumist ja võimaldamist tulevikus[14].

xLaw 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 xLaw kasutamise osas.

Soovitus: kontrollida, millised on täiendavad kulud

EL/NATO liikmesriigis hoitavad andmed

Teenuse suur eelis on, et tegemist on Eesti õigusruumis paikneva firmaga.

xLaw serverid ja andmebaas on majutatud MS Azure pilvtaristul[15]. Peamine piirkond on North Europe (Iirimaa}, varukoopiad tehakse West Europe (Holland} piirkonnas.

Andmete asukoht sõltub seega teenuse infrastruktuurist ja Microsofti serverite asukohtadest.

Soovitus: kontrollida, kas on võimalik valida, kus andmeid hoida

Teenusest lahkumise ja andmete ekspordi võimalus

Kasutaja, kliendi või tema määratud kasutajate poolt rakendusse sisestatud andmete osas (sh väljanõudmise, koopiate tegemise, ülekandmise, kustutamise} kohaldatakse lepingus sätestatut[16].

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

Soovitus: kontrollida võimalust teenusest lahkuda ja eksportida andmeid

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

AI tehnoloogia rakendamisel tuleb lisaks seadusele järgida ka küberturbe ja ühiskondliku ohutuse nõudeid[17].

Infot Extendlaw sertifikaatide kohta ei leidnud. Microsoft Azure ja Office'i

[12] https://www.extendlaw.com/eripakett
[13] https://get.xlaw.eu/#hinnakiri
[14] https://xlaw.eu/tos.html
[15] https://digikogu.taltech.ee/et/itern/52f8b383-9ff0-449f-9000-e01530de05b0
[16] https://xlaw.eu/tos.html
[17] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf

sertifikaadid on leitavad, kuid tõlgendamiseks on vaja teada integratsiooni täpset olemust.

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[18].

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 (artikkel5)[19]. 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

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

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

komponenti (sh selle riskitase) süsteemis kasutatakse [20].

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[21].

Soovitus: kontrollida sertifikaatide olemasolu ja kehtivust

Andmekaitse meetmete rakendamine

Andmekaitse teemasid hõlmavad xLaw teenusetingimused (Terms of Service)[22] ja privaatsuspoliitika (Privacy Policy)[23]. Avalikest allikatest ei nähtu, et xLaw'l oleks andmetöötlusleping, kuid privaatsuspoliitika kohaselt võivad pooled isikuandmete töötlust reguleerida veel pooltevahelises (s.o xLaw ja klient) lepingus.

Teenusetingimuste kohaselt kasutab xLaw küpsiseid, millega kogub erinevaid andmeid. Mh kasutatakse neid andmeid kasutajate loendamiseks ja nende kasutusharjumuste fikseerimiseks turvakaalutlustel ja teenusetingimuste vastavuse kontrolliks.

Teenusetingimustes on sätestatud, et xLaw ei müü ega avalikusta kasutajate isikuandmeid ega kasutajate poolt sisestatud andmeid kolmandatele isikutele (v.a kui on kokku lepitud teisiti)[24].

Teenusetingimused muid üldiseid konfidentsiaalsusklausleid ei sisalda. Samas privaatsuspoliitika kohaselt võib xLaw edastada andmeid kolmandatele osapooltele (privaatsuspoliitikas sätestatud eesmärkidel, mh näiteks maksehäireregistritele).

xLaw töötleb isikuandmeid ainult nõusoleku või seaduse alusel. Samas töötleb xLaw isikuandmeid erinevatel eesmärkidel, sh näiteks lepingu sõlmimisele eelnevateks meetmeteks, rakenduse eesmärgi täitmiseks, kasutajaga suhtlemiseks, teenuse arendamiseks, kliendibaasi haldamiseks, mis võivad omakorda tingida vajaduse teistsuguste õiguslike aluste olemasoluks.

Privaatsuspoliitika kohaselt teavitab xLaw viivitamatult andmete (eelduslikult on mõeldud siiski isikuandmeid) lekkimisest. Täpsemat aega ei ole sätestatud.

Puudub selge teave, kas xLaw edastab isikuandmeid kolmandatesse riikidesse (EL territooriumil paikneva äriühingu puhul saab eeldada, et seadusi järgitakse). Privaatsuspoliitikas välja toodud, et kui xLaw edastab isikuandmeid väljapoole Euroopa Liitu, siis õigusaktides esitatud nõudeid järgides[25].

xLaw säilitab isikuandmeid kuni see on mõistlikult vajalik eesmärgi täitmiseks, milleks neid isikuandmeid töödeldakse või kuni andmesubjekti teistsuguse soovini. Samuti võib xLaw õigustatud huvi alusel säilitada kauem. Säilitustähtaja möödumisel isikuandmed hävitatakse kasutades parimaid praktikaid ja vastavalt xLaw kehtestatud korrale. Privaatsuspoliitikast ei nähtu, kas selle korraga oleks võimalik kusagil tutvuda.

[20] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[21] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[22] https://xlaw.eu/tos.html
[23] https://xlaw.eu/privacypolicy.html
[24] https://xlaw.eu/tos.html
[25] https://xlaw.eu/privacypolicy.html

Alltöötlejate nimekiri ei ole avalikult leitav. See risk vajab kliendi enda käsitlust.

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 üle andmekaitsetingimused

Turvameetmete rakendamine

Teave xLaw kohta on saadud põhiliselt Tallinna Tehnikaülikoolis 2021. a kaitstud magistritööst[26]. Autori sõnul on süsteemi tänane arhitektuur analoogne toonasele, vahepealsete aastate jooksul on lisandunud funktsionaalsusi. Viimase kahe aasta uued funktsioonid on leitavad siit ja kõik funktsioonid siit.

xLaw server ja kasutajaliides on majutatud Azure'i pilve, et sealsete tööriistadega hallata uuendusi, varundamist ja seiret [27].

Kasutajakontode loomine ja integratsioon Oauth 2.0 autentimisteenuste andjatega (Google, Facebook, Microsoft jt} on realiseeritud Firebase Authentication teenuse abil. Kasutajad autendivad end Firebase teenuse vastu (räsitud pääsutalong (token}}, kuid info tellitud paketi ja grupi kohta tuleb xLaw serverist.

Igal kliendil (asutusel, ettevõttel} on oma kasutajate grupp. Kasutaja kommentaare näeb kas ainult ta ise (rakenduse nn kasutajapõhine funktsioon} või kõik temaga samasse gruppi kuuluvad kasutajad ja seda juhtumist sõltumata. Litsentsisaaja kinnitab, et töötleb andmeid õiguspäraselt ehk tema töötaja ei kuritarvita kommentaaride kaudu talle teatavaks saanud teiste, temaga mitte seotud (küll aga samas asutuses käsitletavate} juhtumite infot.

Arendajad ei saa juurdepääsu kasutajate andmetele või kui saavad, kohustab xLaw neid täitma konfidentsiaalsuskohustust[28].

Autentimiseks soovitatakse kasutada OAuth meetodit (näiteks Sign in with Microsoft}, mis võimaldab igal kliendil endal oma kasutajate paroolipoliitikat jmt seadistada ning kasutajatel ei ole vaja eraldi parooli meeles hoida.

Soovitus: kontrollida, kas rakendatud turvameetmed muudavad teenuse ohutumaks

Erinõuded

Nõuded teenustajale: Kõrge riskiga süsteemide puhul peab olema loodud, evitatud, dokumenteeritud ja ajakohaselt hallatud riskijuhtimissüsteem {111 ptk 2. jagu artikkel 9).

Kõrge riskitasemega tehisintellektisüsteeme tuleb arendada, kasutades treenimiseks, valideerimiseks ja testimiseks kvaliteetseid andmekogumeid, mis peavad olema võimalikult asjakohased, vigadeta ja täielikud ning arvestama kasutuse valdkonna spetsiifikat {artikkel 10).

Enne süsteemi turule laskmist või kasutuselevõtmist peab olema koostatud tehniline dokumentatsioon, mida tuleb

[26] https://digikogu.taltech.ee/et/itern/52f8b383-9ff0-449f-9000-e01530de05b0

[27] https://digikogu.taltech.ee/et/itern/52f8b383-9ff0-449f-9000-e01530de05b0

[28] https://xlaw.eu/tos.html

hoida ajakohasena {artikkel 11), vt AI määruse Lisa IV täpsemalt.

Süsteem peab suutma automaatselt salvestada sündmusi kogu oma tööea jooksul, sh selliseid üksikasju nagu, millal seda kasutati, millise andmebaasiga andmeid võrreldi, millised andmed klappisid ning kes on teostanud tulemuste kontrolli {artikkel 12).

Süsteem peab olema loodud läbipaistvana, et kasutajad saaks sellest aru ning oskaks seda õigesti kasutada. Selleks peavad olema selged juhised, mis sisaldavad mh teavet teenustaja, süsteemi võimekuste ja piirangute ning võimalike riskide kohta {artikkel 13).

Kõrge riskiga süsteem peab olema kavandatud viisil, mis võimaldab tõhusat inimjärelevalvet. Järelevalvemeetmed peavad olema proportsionaalsed tehisintellektisüsteemi kasutamisega seotud riskidele ja kontekstile ning sisse ehitatud pakkuja poolt või rakendatavad juurutaja poolt. Järelevalve peab suutma mõista süsteemi võimekusi ja piiranguid, tuvastada ja lahendada probleeme, vältida liigset tuginemist süsteemile, samuti otsustada seda mitte kasutada või selle töö peatada {artikkel 14).

Süsteem peab olema kavandatud täpse, töökindla ja turvalisena ning toimima järjepidevalt kogu oma elutsükli vältel. Kõrge riskiga süsteemi täpsus peab olema näidatud selle kasutusjuhendis.

Nõuded kasutusele võtjale: Nõuded kasutusele võtjale sõltuvad tuvastatud riskitasemest. III ptk 3. jao artikkel 26 kirjeldab kõrge riskitasemega tehisintellektisüsteemide kasutusele võtjate kohustusi. Nende hulka kuuluvad süsteemide kasutamine vastavalt juhistele, inimjärelevalve kehtestamine, sisendandmete asjakohasuse tagamine ja süsteemi toimimise jälgimine. Riski tuvastamisel tuleb sellest viivitamatult teavitada teenustajat ja asjaomaseid ametiasutusi. Kasutusele võtjad peavad säilitama ka AI süsteemi loodud logisid vähemalt kuus kuud. Enne kõrge riskitasemega tehisintellektisüsteemi kasutamist tuleb töötajaid sellest teavitada. Kui süsteem ei ole EL- i andmebaasis registreeritud {VIII ptk artikkel 71), ei tohi seda kasutada. Kasutusele võtjad peavad järgima ka andmekaitsealaseid mõjuhinnanguid ja tegema koostööd asjaomaste ametiasutustega.

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.

AI-ga seotud riskid	**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 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

AI-ga seotud riskid	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

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

xLaw pakub klientidele rohkeid võimalusi, kuidas muuta kasutajate töö produktiivsemaks ja kulutõhusamaks. Samas on vajalik rakendada täiendavaid töökorralduslikke meetmeid ning luua asutusesiseseid protsesse, millega on tagatud turvaline AI kasutamine.

Lisaks tuleb tagada, et asutuse teenuste toimepidevus ei sõltuks ainult xLaw teenuse katkematust tööst.

Vajalik on rakendada täiendavaid meetmeid paralleelselt xLaw kasutamisega, mh koolitada kasutajaid, alternatiivsete töömeetodite arendamine, xLaw kätte saadavate andmete kontrollimine jms. Arvestada tuleks, et AI kasutamise reguleerimine EU tasandil on alles algusfaasis ning puuduvad ka regulatsioonid kohalikul tasandil, mis annaksid selgeid suuniseid AI kasutamiseks.

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