Adobe Firefly

Kirjeldus

Käesolev usaldusväärsuse hinnang keskendub Adobe Inc. pilvtöötlusteenuse (edaspidi Adobe Firefly) riskide kirjeldamisele ning ei kohaldu Adobe Inc. toodetele, mida on võimalik kasutada asutuse sisestel ressurssidel.

Tehisintellekti (artificial intelligence, AI) all mõistame mistahes süsteemi, mis suudab sooritada ülesandeid pealtnäha inimintelligentsi kasutades. Majandus- ja Kommunikatsiooniministeeriumi kratikavad on näinud ette tehisintellekti ulatuslikku rakendamist avalikus sektoris. LLMide (*large language model*) ning difusioonipõhiste pildisünteesimudelite levik ja tavatarbijale kättesaadavamaks muutumine on põhjustanud selles valdkonnas arenguhüppe, sealhulgas AIaaS (artificial intelligence as a service, tehisintellekt teenusena) ärimudeli leviku.

Firefly on teenus, millega saab AI abil luua pilte, videoid, heli ja vektorgraafikat. Firefly pakub AI mudeleid, millega uusi visuaale genereerida.

Adobe asutati 1982. aastal John Warnock and Charles Geschke poolt. Firmas töötab üle 30 000 töötaja üle maailma. 2023. aasta tulu oli 19,41 miljardit USA dollarit. Alates 2007. aastast on Adobe tegevjuhiks Shantanu Narayen[1].

Adobe on 2019. aastal loodud Content Authenticity Initiative'i (CAI) kaasasutaja. Selle initsiatiivi missiooniks on metaandmete standardi loomine digitaalse sisu päritolu kirjeldamiseks ja fikseerimiseks ning seeläbi valeinformatsiooni vastu võitlemiseks.

Firefly on väga edukas projekt, juba esimese kuuga genereeriti 70 miljoni pilti. Adobe'i teenustest Photoshop, Express ja Illustrator käivitatuna on tänaseks Firefly'ga genereeritud enam kui 8 miljardit pilti.[2]

Kasutajate seas on tarkvara hinnatud lihtsalt kasutatava tööriistana, mis aitab kaasa loominguliste ideede genereerimisele ja teostamisele. G2 keskkonnas on teenust hinnatud keskmise hindega 4,6 viiest[3].

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

Teenuse võimalused

SaaS - Adobe Firefly on Uks Adobe poolt pakutavatest teenustest, millega saab AI abil luua pilte (sh vektorgraafikat), videoid ja helisid.[4]

[1] https://www.adobe.com/about-adobe/leaders/shantanu-narayen.html
[2] https://www.adobe.com/ca/about-adobe/fast-facts.html
[3] https://www.g2.com/products/adobe-firefly/reviews
[4] https://www.adobe.com/ee/products/firefly.html

Teenus sisaldab endas erinevaid funktsionaalsusi, milliste kasutamise võimalus oleneb valitud paketist:

- piltide genereerimine tekstist,
- piltide ja vektorgraafika töötlemine (elementide eemaldamine, lisamine ja asendamine tehisintellekti abil),
- lühivideote loomine tehisintellektiga, kasutades tekstiprompti ja pilte,
- heli ja videote tõlkimine,
- heliefektide loomine,
- Firefly tahvel.

Adobe Firefly kasutab Adobe enda treenitud AI mudeleid. Treenimiseks kasutavad nad andmestikke, millele neil on õigus {nt Adobe Stock), mis on avalikud või mille autoriõigus on aegunud. Klientide andmeid nad oma mudelite treenimiseks ei kasuta[5].

Lisaks omatreenitud mudelitele on Adobe toodetesse integreeritud ka partnerite mudelid.[6] Fireflyd on võimalik kasutada ka mobiiliäpis.[7]

Soovitus: kontrollida, et integreeritud partnerid oleksid usaldusväärsed

Kasutusjuhud

Standardloetelu viisidest, kuidas teenust saab kasutada:

- visuaalide (pildid, videod, vektorgraafika) genereerimine;
- kõne tõlkimine;
- heliefektide loomine;
- visuaalide töötlemine.

EL tehisintellekti määruse kohane riskitase

Teenuse kasutamine vastavalt kirjeldatud tootlusjuhtudele liigitub minimaalse riskiga tehisintellektiks.

Kasutajatele tuleb selgitada, mis tingimustel on lubatav üles laadida fotot tundmatust inimesest (isikuandmed).

Soovitus: kontrollida, et kasutajad ei laeks teenusesse isikuandmeid

Rahaline mõju

Pakett Firefly Free on kõigile kasutajatele tasuta ning selle paketiga on võimalik genereerida pilte, videoid ja heli; kasutaja loovkrediidi generative credit kogus on piiratud (täpset kogust ei ole nende lehel täpsustatud).

Pakett Firefly Standard maksab 11,45 eurot kuus. Selle paketiga saab 2000 ühikut igakuist loovkrediiti kuus. Samuti saab piiramatu juurdepääsu tavalistele pildi- ja vektorfunktsioonidele, võimaluse luua kuni 20 viiesekundilist videot ja tõlkida kuni 6 minutit heli või videot.

Pakett Firefly Pro maksab 34,37 eurot kuus. Selle paketiga saab 7000 ühikut igakuist loovkrediiti. Samuti saab piiramatu juurdepääsu tavalistele pildi- ja vektorfunktsioonidele, võimaluse luua kuni 70 viiesekundilist videot ja tõlkida kuni 23 minutit heli või videot.

Pakett Firefly Premium maksab 229,23 eurot kuus. Selle paketiga saab 50 000 ühikut igakuist loovkrediiti. Samuti saab piiramatu juurdepääsu tavalistele pildi- ja vektorfunktsioonidele, piiramatu juurdepääsu Firefly videomudelitele

[5] https://www.adobe.com/ai/overview/firefly/gen-ai-approach.html
[6] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-partner-models-security-fact-sheet.pdf
[7] https://www.adobe.com/ee/products/firefly.html

videote genereerimiseks ja võimaluse tõlkida kuni 166 minutit heli või videot.

Pakette on võimalik võtta ka meeskondadele. Sellisel juhul jäävad pakettide tingimused samaks, aga lepingud on aastased ning arveid esitatakse igakuiselt. Paketi Firefly Standard puhul on siis hind 9,23 eurot kuus litsentsi kohta. Paketi Firefly Pro puhul on hind 27,7 2 eurot kuus litsentsi kohta. Paketi Firefly Premium puhul on hind 184,86 eurot kuus litsentsi kohta.

Leidub ka pakett nimega Creative Cloud Pro, mille puhul on võimalik kasutada 20 Adobe teenust. Firefly puhul saab kasutaja iga kuu 4000 ühikut loovkrediiti, luua kuni 40 viiesekundilist videot ja tõlkida kuni 12 minutit heli või videot. See pakett maksab 81,27 eurot kuus. Tudengitele ja õpetajatele maksab 25 eurot kuus (esimese aasta hind, järgmine aasta 41,66 eurot kuus), meeskondade puhul on hind 86,55 eurot kuus litsentsi kohta[8].

Adobe Firefly 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 Adobe Firefly kasutamise osas.

Garanteeritud minimaalne aktiivaeg (uptime) Adobe teenustele on 99,9%. Kui ühe kalendrikuu jooksul on teenuse aktiivaeg alla 99,9%, siis on kliendil võimalik saada Service Creditit ja sellega on võimalik vahendada oma kuumaksumust vastavalt aktiivajale[9].

- Kui aktiivaeg oli 99,5% ja <99,9%, siis on võimalik saada 5% maha kuutasudest.
- Kui aktiivaeg oli95,0% ja <99,5%, siis on võimalik saada 10% maha kuutasudest.
- Kui aktiivaeg oli90,0% ja <95,0%, siis on võimalik saada 15% maha kuutasudest.
- Kui aktiivaeg oli <90,0%, siis on võimalik saada 25% maha kuutasudest.

Adobe'i kõigi teenuste seisu kuvatakse veebilehel[10] ning konkreetselt Firefly teenuse seisu lehel[11].

EL/NATO liikmesriigis hoitavad andmed

Adobe töötleb, hoiab vahemälus ja potentsiaalselt talletab Firefly sisendteavet AWS andmekeskustes, mis asuvad Ameerika Ühendriikides (Oregon, Virginia). [Firefly talletab genereerimistega seotud teavet Ameerika Ühendriikides (Virginia), lirimaal ja Jaapanis. Adobe talletab hüvitistega seotud infot oma litsentside andmebaasis, mis asub lirimaal.[12]

Firefly pakub mitmeid rakendusliideseid (AP/d). Peamiselt Firefly APIsid kaitatakse AWS andmekeskustes, mis asuvad Ameerika Ühendriikides (Oregon, Virginia). Heli ja video APId kasutavad lirimaa servereid, aga töötlus toimub ikkagi Ameerika Ühendriikides. lnDesing APId kasutavad Azure ja AWS andmekeskusi Ameerika Ühendriikides. Azure AI Translator Service puhul toimub töötlus Ameerika Ühendriikides.[13]

Ettevõte talletab genereeritud sisu (Generation History) oma AWS taristul

[8]https://www.adobe.com/products/firefly/plans.html

[9]https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/SLA-AdobeOn-demand-ManagedServices25FEB2022.pdf

[10]https://status.adobe.com/cloud/creative_cloud#/

[11]https://status.adobe.com/products/536716

[12]https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[13]https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-services-security-fact-sheet.Pdf

olevais andmekeskustes (Enterprise Storage) USAs, Iirimaal ning Jaapanis[14].

Soovitus: kontrollida, kus andmeid majutatakse ning varundatakse

Teenusest lahkumise ja andmete ekspordi võimalus

Teenuse kasutamisele asudes saab kasutaja oma arvutis määrata kataloogi Firefly sisendandmete tarbeks. Pildid, mille alusel Firefly genereerib uusi visuaale, võetakse sellest kataloogist. Alates 2025. aasta märtsist võib sääraseks "lokaalseks asukohaks" olla ka Adobe Enterprise Storage, Amazon Web Services {AWS), Azure, Dropbox voi Google Drive.
Kui Firefly kasutab etteantud materjale, siis teatud funktsionaalsuste jaoks hoitakse neid materjale AWSi serverites 24 tundi ja seejärel kustutatakse.

Firefly poolt genereeritud materjale hoitakse AWS serverites ning kasutajale tagastatakse viit (URL) loodud sisule.
Kui soovitakse kasutada tehisintellektiväliseid võimalusi, (nt Photoshop, Premier Pro, lnDesign ja Lightroom), siis töötlemiseks kasutatavaid pilte ja sisu hoitakse töötlemise hetkel ainult vahemälus ning need kustutatakse töötluse lõppedes.[15]

Firefly kasutab genereeritud sisu säilitamisel mitut käitumisviisi. Sisu, mis on salvestatud veebilehitseja lemmikutesse (browser-saved favourites), kustutatakse mingi aja pärast pöördumatult[16].

Varundamiseks peab kasutaja selle sisu ise alla laadima. Funktsionaalsustega Text to Image ja Generate video loodud sisu hoitakse teenuse kasutamise ajaloos (Generation history) ning see on kättesaadav ka hiljem.

Genereeritud sisu autorsuse ja päritolu tõendamiseks loob Adobe sellele sisumandaadi Content Credentials, seda hoitakse nii sisu enda juures manusena kui talletatuna vastavasse hoidlasse.

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

Soovitus: kontrollida, kui kaua teenusepakkuja andmeid säilitab

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

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

Adobe on saavutanud vastavuse järgmiste standarditega: SOC 2, ISO 27001, PCI ja FedRAMP. Täieliku ülevaate sertifikaatidest leiab Adobe kodulehelt[18],

[14] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/ adobe-firefly-fact-sheet.pdf
[15] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-services-security-fact-sheet.pdf
[16] https://helpx.adobe.com/firefly/web/view-history/view-generation-history/view-generation-history.html
[17] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[18] https://www.adobe.com/trust/compliance/compliance-list.html

seda nimekirja täiendatakse ja uuendatakse pidevalt.

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[19].

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)[20]. 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

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

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

komponenti (sh selle riskitase) süsteemis kasutatakse [21].

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[22].

Soovitus: kontrollida, kas teenusepakkuja sertifikaadid vastavad KüTS nõuetele

Andmekaitse meetmete rakendamine

Andmetöötlust reguleerivad peamiselt Adobe üldised kasutustingimused[23] (Adobe General Terms of Use, NB! ebaselguse korral tuleb juhinduda ingliskeelsetest tingimustest), tootepõhised tingimused[24], privaatsuspoliitika[25], andmetöötlusleping[26] (Data Processing Addendum) ja andmekaitsetingimused[27]. NB! andmetöötluslepingu puhul tuleb kontrollida, et tegemist oleks õige versiooniga (genereeritakse parast sisselogimist). Viidatud lisa on leitud otsinguga Adobe'i veebilehelt.

Üldiste kasutustingimuste kohaselt kohaldub:

- andmetöötlusleping juhul, kui töödeldakse Euroopa Majanduspiirkonna üksikisikute isikuandmeid
- andmekaitsetingimused juhul, kui isikuandmed on seotud isikutega väljaspool Euroopa Majanduspiirkonda.

Lisaks on olemas Adobe privaatsuspoliitika, mis võib samuti teatud juhtudel äriklientide kasutajatele kohalduda (kui Adobe on vastutav töötleja, nt juhul kui Adobe kogub ärikliendi kasutajate kasutusandmeid). Seega tuleb enne Adobe Firefly kasutuselevõttu täiendavalt analüüsida ka privaatsuspoliitikat, et klient saaks oma kasutajatele anda piisavalt teavet andmetöötluse asjaolude kohta ning et andmetöötlus oleks kooskõlas kohalduvate õigusaktidega.

Üldiste kasutustingimuste kohaselt nõustub klient mitte töötlema tundlikke isikuandmeid (Sensitive Personal Information, termini täpsustuse leiab üldistest kasutustingimustest) välja arvatud, kui Adobe on andnud selleks otsese loa, see on teenuste ja tarkvaraga ette nähtud või seda näevad ette tootepõhised tingimused, kui neid kohaldatakse.

Üldistes kasutustingimustes on täpsustatud, millistel juhtudel on Adobe'l juurdepääskliendiandmetele ja millal Adobe seda võimalust kasutab.

Adobe edastab andmeid kolmandatesse riikidesse.

Adobe ei kasuta kliendisisu Adobe turunduseks ega reklaamimiseks. Samuti ei kasuta Adobe kliendiandmeid generatiivse tehisintellekti treenimiseks.

Sisuanalüütika (Content Analytics) on vaikimisi sisse lülitatud, selles osalemisest

[21] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[22] https://www.ria.ee/sites/default/files/documents/2024-03/Tehisintellekti-masinoppe-tehnoloogia-riskide-uuring-2024.pdf
[23] https://www.adobe.com/legal/terms.html
[24] https://www.images2.adobe.com/content/dam/cc/en/legal/servicetou/adobe-generative-ai-product-specific-terms-en-us-20250617.pdf
[25] https://www.adobe.com/privacy/policy.html
[26] https://www.adobe.com/cc-shared/assets/pdf/legal/ terms/enterprise/pdfs/dpa-ww.pdf
[27] https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdfs/DPT-WW.pdf

loobumiseks peab klient ise samme astuma.

Kui klient kasutab Adobe salvestusruumi, siis litsentsi lõppemisel jätab Adobe endale õiguse kliendi andmed kustutada.[28]

Adobe ei kombineeri isikuandmeid mujalt saadud isikuandmetega ega töötle isikuandmeid väljaspool kliendi ja Adobe vahelist ärisuhet, v.a kui see ei tulene pooltevahelisest lepingust. Adobe ei müü ega jaga isikuandmeid (arvestades nende mõistete tähendust CCPA või muude USA õigusaktide järgi).

Adobe teavitab klienti isikuandmetega seotud rikkumisest põhjendamatu viivituseta. Täpsemat aega ei ole kokku lepitud.

Teenuste kasutamise lepingu lõppemisel Adobe kustutab või tagastab isikuandmed (kliendi valikul)[29]. Andmete säilitamise tähtaegu on Adobe selgitanud veebilehel olevas Security Fact Sheet: Adobe Firefly for Enterprise dokumendis[30] (lk 8).

Alltöötlejate nimekiri on leitav veebilehelt: https://www.adobe.com/privacy/sub-processors.htm1. Selle nimekirja kohaselt edastab Adobe andmeid kolmandatesse riikidesse.

Adobe andmekaitsetingimused (kohaldumist vt eelnevast)[31] ei ole nii põhjalikud kui andmetöötlusleping ning sõltuvalt töödeldavatest isikuandmetest tuleb hinnata, kas tingimused on piisavad.

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 riikidesse teenusepakkuja andmeid võib edastada

Erinõuded

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

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

Üldiste kasutustingimuste kohaselt nõustub klient mitte töötlema tundlikke isikuandmeid (Adobe üldised kasutustingimused) välja arvatud, kui Adobe on andnud selleks otsese loa, see on teenuste ja tarkvaraga ette nähtud või seda näevad ette tootepõhised tingimused, kui neid kohaldatakse[32].

Klient vastutab üleslaaditud materjalide eest täielikult ning ei tohi üles laadida järgmisi materjale[33]:

- kaubamärgiga kaitstud;
- sisu, mis sarnaneb autoriõigustega kaitstud materjalidega;
- isikuandmeid sisaldavaid materjale;

[28] https://www.adobe.com/legal/terms.html
[29] https://www.adobe.com/cc-shared/assets/pdf/legal/terms/enterprise/pdfs/dpa-ww.pdf
[30] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whi tepapers/creative-cloud/adobe-firefly-fact-sheet.pdf
[31] https://www.adobe.com/content/dam/cc/en/legal/terms/enterprise/pdf s/DPT-WW.pdf
[32] https://www.adobe.com/legal/terms.html
[33] https://www.images2.adobe.com/content/dam/cc/en/legal/servicetou/adobe-generative-ai-product-specific-terms-en-us-20250617.pdf

- materjale, mis on vastuolus seadustega;
- materjale, mis on vastuolus Adobe kasutustingimustega;

Adobe tehisintellektiteenusesse ei tohi klient sisestada isikuandmeid, kui see ei ole kooskõlas kohalduva õigusega (mh isikuandmete kaitse õigusaktidega).

Täpsem ja pikem nimekiri nõuetest, mida klient peab AI teenuseid kasutades järgima, on leitav Adobe kodulehel.

Klient peab ise veenduma, et Firefly vahendusel kasutatavate partnermudelite kasutustingimused on talle vastuvõetavad[34].

Soovitus: kontrollida, millised on partnermudelite kasutustingimused

Turvameetmete rakendamine

Arendustöös juhindub Adobe turvalise tootearenduse elutsüklist[35]. Teenuse käigushoidmisel rakendatud korralduslikud (operational) meetmed on kirjeldatud.[36]

Andmeid (identiteediandmed, prompt, kontekst (reference context)) liigutatakse sidekanalis krüpteeritult (TLS 1.2 v6i kõrgem) ja on krüpteeritud AES-128- GCM algoritmiga[37]. Partnerite mudelite kasutamise korral on andmed (sh identiteediandmed) jõudeolekus krüpteeritud AES-256 algoritmiga[38].

Juurdepääse hallatakse Adobe identiteedihaldusteenustega (Adobe Identity Management Services, IMS), mida on SSO abil võimalik liidestada kliendi identiteedihalduriga. Igal kasutajal on unikaalne identifikaator (named user licensing), mille eesmärk on sisu autorsuse ja päritolu tõendamine (vt AI06, Content Credentials). Identiteedi tüüpe saab olla erinevaid, hallata saab neid käsitsi või automatiseeritult[39].

Töökindluse tagamiseks replitseeritakse identiteediandmed Põhja-Ameerika, Euroopa ja APAC- i andmekeskustesse ja seda sõltumata kliendi asukohast.

Firefly Services toetab serveritevahelist OAuth autentimist[40]. Nõrkuste avaldamise programm ja veaotsingu tasuprogramm on mõeldud ka AI - spetsiifiliste nõrkuste leidmiseks[41].

Avalikes allikates ei leidunud infot FireFly AI-spetsiifiliste nõrkuste kohta.

Adobe kasutab oma mudelite treenimiseks andmestikke, millele ettevõttel on õigused {nt modereeritud pildid Adobe Stockist), mis on avalikud või mille autoriõigus on

[34] https://www.adobe.com/cc -shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-partner-models-security-fact-sheet.pdf

[35] https://www.adobe.com/cc-shared/assets/pdf/trust/adb-application-security-overview.pdf

[36] https://www.adobe.com/cc-shared/assets/pdf/trust/adobe-operational-security-overview.pdf

[37] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-fact-sheet.pdf

[38] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-partner-models-security-fact-sheet.pdf

[39] https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/corporate/adobe-identity-management-services-security-overview.pdf

[40] https://www.adobe.com/content/dam/cc/en/trust-center/ungated/whitepapers/creative-cloud/adobe-firefly-services-security-fact-sheet.pdf

[41] https://blog.adobe.com/en/publish/2024/05/01/adobe-collaborates-with-ethical-hackers-build-safer-more-secure-ai-tools

aegunud. Klientide andmeid nende mudelite treenimiseks ei kasutata[42]. Ettevõte väidab, et nende mudelid ei genereeri sisu, mis rikub autoriõigust või intellektuaalomandi õigusi ning nende mudelid on ohutud ka ärilistel või hariduslikel eesmärkidel kasutamiseks. Enterprise klientidele pakutakse hüvitist (indemnification option) juhul kui FireFly toodangust peaks tõusma intellektuaalomandivaidlus.

Adobe testib oma mudeleid pidevalt, avastamaks potentsiaalset kallutatust või stereotüüpe. Kasutajatel on võimalik anda tagasisidet, kui nad juhtuvad sedasorti olukordi märkama[43].

Ettevõttel on AI eetika põhimõtted[44] [45] ja koos käib AI eetika nõukogu (A/ Ethics Review Board). AI funktsioonidele koostavad nende arendajad AI eetika mõjuhinnangu, et tuvastamaks kahjulikku kallutatust ja stereotüüpe.

Genereeritud sisule lisab Adobe Content Credentials funktsiooniga sildi järgneva teabega: kasutaja GUID, sisu loomise ja muutmise aeg, mudel, tulemist ja selle metaandmetest arvutatud räsi ning teatud juhtudel ka pisipildi (thumbnail), kas tulemus on loodud algusest peale FireFly's või on loodud kombineerimise teel mujalt pärit sisuga, kokkuvõte FireFly's sooritatud tegevustest[46]. See silt talletatakse lisaks sisule ka vastavas hoidlas Content Credentials repository. Töökindluse tagamiseks on viimane majutatud AWS US-East piirkonna andmekeskustesse (sõltumata kliendi asukohast).

Partnerite mudelite puhul on Adobe seisukoht, et mudeli kahjulikkuse ja kallutatuse testimise eest vastutab mudeli tootja/pakkuja; Adobe ise partnerite sellekohaseid tõendeid ei valideeri[47].

Soovitus: kontrollida, et teenusepakkuja ei rikuks intellektuaalomandiõigusi

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

[42] https://www.adobe.com/ai/overview/firefly/gen-ai-approach.html
[43] https://www.adobe.com/ee/products/firefly.html
[44] https://www.adobe.com/about-adobe/ethicsandintegrity.html
[45] https://www.adobe.com/ee/ai/overview/ethics.html
[46] https://helpx.adobe.com/creative-cloud/apps/adobe-content-authenticity/content-credentials/overview.html
[47] https://www.adobe.com/cc-shared/assets/pdf/trust-center/ungated/whitepapers/creative-cloud/adobe-partner-models-security-fact-sheet.pdf

AI-ga seotud riskid	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 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.**

AI-ga seotud riskid	
	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

Adobe on rakendanud infoturbe ja andmekaitse alaseid meetmeid, millega saab lugeda Adobe Firefly teenus usaldusväärseks. Adobe andmete majutab andmeid Ameerika Ühendriikides ja mujal maailmas aga andmete töötlus toimub Ameerika Ühendriikides, mistõttu ei ole tagatud andmekaitsenõuete täitmine.

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

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