Eleri Pilliroog

From: Eleri Pilliroog
Sent: neljapäev, 2. jaanuar 2025 10:39
To: 'Ralf Mägi'
Subject: RE: AI automatsioon meilboksis

Categories: Tehnoloogia

Tere!

Olete pöördunud AKI poole saamaks õiguslikku hinnangut Teie tehisintellektil põhineval lahendusele seoses isikuandmete töötlemisega.

Inspektsioon annab siduvaid õiguslikke hinnanguid üksnes järelevalve menetluse käigus. Kuna hetkel menetlust alustatud ei ole, ei saa me kõiki asjaolusid teadmata eelhinnangut anda.

Nagu ennist telefonis ütlesin on andmetöötleja enda kohustus ise analüüsida, kas ja millisel õiguslikul alusel on võimalik andmetöötlust läbi viia. Õigusliku aluste kohta saate lugeda siit:
https://www.aki.ee/isikuandmed/andmetootlejale/tootlemise-oiguslikud-alused

Lisaks määrab isikuandmete kaitse üldmäärus veel ka teisi kohustusi, mida peab järgima isikuandmete töötlemisel nt läbipaistvus, minimaalsus jne. Täpsemalt siin: https://www.aki.ee/isikuandmed/andmetootlejale/andmetootluse-pohimotted
ja siin: https://www.aki.ee/isikuandmed/juhendid/isikuandmete-tootleja-uldjuhend

2. augustil 2024 jõustus ka Euroopa Liidu AI määrus. See sätestab ühetaolise reeglistiku tehisintellektisüsteemide arendamisele ja kasutamisele. Määruse keskne eesmärk on tagada inimeste tervise, ohutuse ja põhiõiguste kaitse ning edendada seda, et tehisintellekti üha ulatuslikum kasutamine ühiskonnas püsiks inimkeskne ja usaldusväärne. Palume Teil vajadusel sellega tutvuda ning võtta arvesse sellest määrusest tulenevaid kohustusi.

Lugupidamisega

Eleri Pilliroog
Andmeturbe ekspert
eleri.pilliroog@aki.ee

ERAELU KAITSE JA RIIGI LÄBIPAISTVUSE EEST
Tatari 39 | 10134 Tallinn | Eesti
LinkedIn I Youtube

From: Ralf Mägi <ralf.m2gi@gmail.com>
Sent: Saturday, December 21, 2024 1:02 PM
To: Eleri Pilliroog <Eleri.Pilliroog@aki.ee>
Subject: Re: AI automatsioon meilboksis

Tere jälle!

Vabandan, ei taha Teid asjata kiirustada, aga oleksin väga tänulik Teie arvamuse eest! :)

Kiire update ka:

Ühe ettevõttega arutasime ka, et võivad ostutingimustesse lisada, et andmeid jagatakse OpenAI-ga ja sellele peab linnukese andma enne tellimuse tegemist.
Ehk kui tellimuse sooritanud klient tuleb infot küsima meili teel oma andmetega, oleks see vist okei.

Kuid jällegi, mida teha, kui neile kirjutab inimene, kes pole klient ja lisab oma andmeid meili, mida jagatakse koheselt OpenAI-ga, sest 100% puhastada pole võimalik?

Parimate soovidega
Ralf Mägi

Kontakt Ralf Mägi (<ralf.m2gi@gmail.com>) kirjutas kuupäeval T, 17. detsember 2024 kell 15:12:

> Tere, Eleri!
>
> Tänud abi eest eelmisel korral!
>
> Siin on kiire meeldetuletus projektist. Nimelt ehitan ettevõtetele klienditeeninduse meilide automatiseerimiseks AI süsteemi. Projektid on algusjärgus ning seisavad GDPR probleemi taga.
>
> Väga lihtsustatult:
>
> 1. Minu server on ühendatud ettevõtte klienditeeninduse meilboksiga ning kuulab meilboksi.
> 2. Iga kord, kui uus kiri klienditeenindusse tuleb, näeb minu server kirja.
> 3. Minu server võtab terve emaili vestluse ning eesmärk on sellele vastus genereerida.
> 4. AI genereeritud vastus pannakse mustandina kirja meilboksi. Teenindaja vaatab üle ja saab vastuse ära saata.
>
> Probleem on aga selles, et meili sisu on vaja jagada OpenAI-ga. Enne jagamist peaksime meilivestlused anonümiseerima, sest tegelikult ei ole vaja privaatseid andmeid vastuse genereerimiseks kasutada.
>
> Kahjuks on privaatandmetest vestluste puhastamine väga keeruline (eesti aadressid, telefoninumbrid ja nimed) ning lõpuks liiga ebatäpne. Tähendab, et kui süsteem tööle tahta saada, on siiski vaja kliendiandmeid mingi määrani jagada.
>
> Kliendilt nõusolekut ei ole võimalik küsida, sest nad saadavad lihtsalt meili oma andmetega.
>
> Kas oskate ehk kommenteerida, kuidas asjaga edasi minna, kui meilidest ei saa eesti keelseid privaatandmeid hästi eemaldada (väga töömahukas, veamäär oleks lõpuks liiga kõrge) ning nõusolekut samuti küsida ei saa.
>
> **1. Kas oleks siiski võimalik õigustatud huvi variandiga edasi minna?**
> Lahendus teeks klienditeeninduse töö palju mugavamaks, lõpptarbijale kiiremaks ning samuti annaksime endast maksimumi, et kliendiandmete jagamist minimaliseerida.
>
> Tulevikus võib aga nende jagamine ka osa kordadest põhjendatud olla, näiteks tellimuse infole saaks AI agent ligi kliendiandmeid kasutades. Siis tekib aga omakorda probleem, et kuidas tuvastada süsteemiga, millise meili puhul on andmete jagamine õigustatud ning millal on see ebavajalik.

2. Kuidas määrata ära, kas oleme teinud piisavalt, et andmete jagamist minimaliseerida? Milline veamäär on okei?

Suur tänu ette!

Parimate soovidega
Ralf Mägi
Verbotica OÜ