Översiktlig bedömning av OpenAI:s Chat GPT, DALL-E m.fl. 2023-05-08

Bakgrund

Licensfunktionen på KTH VS/IT har fått in ett antal inköpsärenden där forskare och andra anställda på myndigheten vill köpa licenser för Chat GPT, DALL-E m.fl. tjänster från OpenAI.

IT-SMC har därför gjort en översiktlig bedömning för att kunna ge vägledning.

Dokumentation till underlag för bedömningen

Avtal och villkor:

- https://openai.com/policies/terms-of-use
- https://openai.com/policies/privacy-policy
- https://openai.com/policies/data-processing-addendum
- record-Data Processing Agreement (KTH and OpenAI).pdf
  - Ett automatgenererat avtalsförslag från deras avtalstjänst, där vi sedan avbröt processen innan vi ingick någon överenskommelse
- OpenAI Information Security Addendum in DPA - Exhibit B ANNEX II
  - Vi skickade en förfrågan till legal@openai.com för att få ta del av dokumentet och de skickade OpenAI Information Security Addendum (March 2023).pdf
- https://platform.openai.com/subprocessors

Hur OpenAI använder data som behandlas i tjänsten:

- https://platform.openai.com/docs/data-usage-policies
- https://help.openai.com/en/articles/7039943-data-usage-for-consumer-services-faq
- https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance

OpenAI i Microsoft Azure:

- https://learn.microsoft.com/en-us/legal/cognitive-services/openai/limited-access
- https://azure.microsoft.com/en-us/products/cognitive-services/openai-service/#overview
- https://learn.microsoft.com/en-us/azure/cognitive-services/openai/overview#comparing-azure-openai-and-openai
- https://learn.microsoft.com/en-us/azure/cognitive-services/openai/quickstart?tabs=command-line&pivots=programming-language-studio
- https://customervoice.microsoft.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbR7en2Ais5pxKtso_Pz4b1_xUOFA5Qk1UWDRBMjg0WFhPMkIzTzhKQ1dWNyQlQCN0PWcu
- https://learn.microsoft.com/en-us/azure/cognitive-services/openai/faq
- https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy
- https://customervoice.microsoft.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbR7en2Ais5pxKtso_Pz4b1_xURE01NDY1OUhBRzQ3MkQxMUhZSE1ZUlJKTiQlQCN0PWcu

Bedömning

OpenAI delar upp sitt erbjudande i konsumenttjänster och kommersiella tjänster med väsentligt olika förhållningssätt till vad som gäller för det data som hanteras i dem.

Personuppgiftsbiträdesavtal och behandling av personuppgifter

Konsumenttjänster (ChatGPT, DALL-E)	Kommersiella tjänster (API)
Det går inte att teckna något personuppgiftsbiträdesavtal med EU:s standardkontraktsklausuler för det OpenAI benämner som sina konsumenttjänster: ” (ChatGPT, DALL-E Labs)”. Det innebär att KTH inte kan behandla personuppgifter i de tjänsterna utan att bryta mot dataskyddsförordningen.	Det går däremot att teckna personuppgiftsbiträdesavtal med EU:s standardkontraktsklausuler för det OpenAI benämner som sina kommersiella tjänster: ”… business service offerings (APIs for text completion, images, embeddings, moderations, etc.)”. Notera att det är delegationsordningen som reglerar vem som får ingå avtal för KTH:s räkning samt att avtalen ska diarieföras. All behandling sker i 3:e land (USA). Ingår KTH deras personuppgiftsbiträdesavtal accepterar vi deras nuvarande underbiträden. De informerar om förändringar i vilka underbiträden de använder och det finns möjlighet ett bryta avtalet om vi inte accepterar dem. Det finns också skrivningar om att de kan försöka adressera invändningarna, men bedömningen är att det är osannolikt att det sker för enskilda kunders invändningar. Notera att OpenAI ställer flera krav på KTH som kund under ” 6. Obligations of Customer.”, bl.a. att: • KTH:s åliggande omfattar, men är inte begränsat till, att föra register över ”completion ID” eller motsv. ID-nummer som är relaterade till specifika registerade för att kunna ge stöd till OpenAI när de ska hantera individer som vill utöva sina rättigheter som registerade enl. GDPR. • KTH ska säkerställa att dataskyddsförordningen och andra lagar kring dataskydd följs. Notera också att det explicit framgår i personuppgiftsbiträdesavtalet under B. DESCRIPTION OF TRANSFER att inga känsliga personuppgifter förväntas föras över för

	behandling ifall inte användaren oväntat inkluderar sådana uppgifter i ostrukturerat data.

Tystnadsplikt

OpenAI refererar i flera av dokumenten till att deras och deras underbiträdens personal med tillgång till kunddata omfattas av kommersiell, avtalsreglerad, tystnadsplikt och särskilda säkerhetsreglementen.

Användning av data för träning

Konsumenttjänster (ChatGPT, DALL-E)	Kommersiella tjänster (API)
För konsumenttjänsterna tränar de sina modeller på kunddata per default. Det går att göra opt-out via ett webbformulär. OpenAI beskriver också 4 scenarios där auktoriserad personal hos dem tar del av data som behandlas i tjänsten: 1) säkerhets- eller abuseärenden, 2) supportärenden, 3) för att uppfylla rättsliga krav och 4) vid modellträning (om vi inte gjort opt-out).	OpenAI ändrade praxis för sina kommersiella API-tjänster från och med 1:a mars 2023 och använder per default inte längre data kunder exponerar för dem via API:et för att träna sina modeller. De sparar data i 30 dagar för att hantera abuse-ärenden och skadlig användning. En liten grupp auktoriserad personal hos OpenAI och deras underleverantörer kan komma att ta del av det datat vid utredning av sådana fall. De nämner möjligheten att avtala bort detta för enterprise-kunder under vissa förutsättningar när risken för abuse eller missbruk är låg. Gör vi opt-in för modellträning för API-användning så har sannolikt viss OpenAI-personal till datat. Bedömningen är att de dessutom har tillgång till datat för att uppfylla rättsliga krav och vid supportärenden.

Intellektuella rättigheter, skyddsvärt data, ägarskap

Data som förs över för behandling hos OpenAI hanteras i 3:e land och kan komma att hanteras av personal hos OpenAI eller deras underbiträden.

Enligt OpenAI:s Terms of Use, 3. Content (a) Your Content, äger KTH sitt ”Input” och får rättigheterna till sitt ”Output”. KTH accepterar samtidigt att OpenAI får använda ”Content” (”Input” och Output” sammantaget) för att tillhandhålla och underhålla tjänsten, möta rättsliga krav och upprätthålla sina policies.

Not om Azure OpenAI Service

Vid bedömningen av OpenAI:s tjänster noterade vi att Azure OpenAI Service erbjuder API-access till OpenAI:s Language Models i Azure med möjlighet att behandla informationen inom EU/EES. För närvarande krävs dock att kunden ansöker om tillgång till Azure OpenAI Service för sitt användningsscenario.

Azure OpenAI Services tränar inte sina modeller på data kunden exponerar via API:et.

Prompts och Completions lagras i 30 dagar och monitoreras av Microsofts personal i syfte att upptäcka användning som står i strid med användningsvillkoren. Det går att ansöka om undantag från monitorering.

KTH har redan personuppgiftsbiträdesavtal med Microsoft som omfattar Azure. Kommersiell, avtalsreglerad tystnadsplikt för Microsofts personal och deras underbiträden är del av KTH:s avtal med Microsoft.

Bedömning och vägledning

- Ska personuppgifter behandlas är endast OpenAI:s API-tjänst möjlig att använda
    - Det ska göras en konsekvensbedömning, https://intra.kth.se/anstallning/anstallningsvillkor/att-vara-statligt-an/behandling-av-person/konsekvensbedomningar-for-behandling-av-personuppgifter-1.1151189
    - Det måste tecknas ett personuppgiftsbiträdesavtal
    - Undvik att hantera känsliga personuppgifter
    - Notera det ansvar som ligger på er som använder API-tjänsten om ni hanterar personuppgifter för registrerade där
- Undvik att exponera skyddsvärd information, t.ex. sådant som kan leda till patent eller skulle medföra skada eller ekonomiskt bortfall för KTH ifall informationen kom i andras händer
- *Har ni möjlighet att få tillgång till Azure OpenAI Services, så är vår bedömning att det är det bättre alternativet ur efterlevnadsperspektiv – vägledningen ovan (för OpenAI) gäller även Azure OpenAI Services*

Vid en väsentlig förändring i tjänsten eller i hur tjänsten ska användas, så behöver en ny bedömning göras. Detsamma gäller vid förändringar i lagar, förordningar eller utlåtanden från tillsynsmyndigheter som påverkar förutsättningarna för att använda tjänsten.

2023-05-08

IT-SMC <it-smc@kth.se>,

KTH GVS/IT/IT-Stab