Appendix 1 – ChatGPT - AI product assessment

1. General information
    a) **AI product name**: ChatGPT, OpenAI AI Assistant
    b) **Intended use-case**: AI assistant for text and information processing within the company
    c) **Date**: 13/03/2025
    d) **Product URL**: https://chatgpt.com/ , https://chat.openai.com/
    e) **Link to privacy policy**: link
    f) **Functional documentation**: link
2. Purpose and Scope
    a) **Objective of the AI product**: to provide an AI assistant for text-based tasks and information retrieval within the company, internet or AI model knowledge[1].
    b) **What is the problem that AI product resolve**: to potentially enhance employee productivity, assist with information processing, and streamline text-related workflows within the company.
    c) **Who are the primary users**: internal employees
    d) **Expected impact on employees and clients**: potential for increased efficiency and access to information for employees. Potentially, unnatural communication message if employees use product for communicating with clients through e-mails, communicators or documents. Distorted communication in cases where there is not human control.
3. Compliance
    a) **Regulatory considerations**: GDPR[2], SOC2[3], and SCC[4]. OpenAI states that they and the Customer each agree to comply with their respective obligations under applicable data privacy and data protection laws, including GDPR and U.S. Privacy Laws. For customers located in the EEA or Switzerland, OpenAI Ireland Ltd. provides the Services. OpenAI also utilizes Standard Contractual Clauses (SCCs) for international data transfers. Personal Data or any data placed into ChatGPT may to be reviled into vendors and service providers of OpenAI, or Gov Authorities or other third parties listed on OpenAI regulations.
    b) **Security considerations**: security is essential to OpenAI's mission. They value input from security researchers. OpenAI has a Bug Bounty Program to reward security researchers for finding vulnerabilities[5]. They also maintain reasonable

[1] ChatGPT Capabilities Overview, OpenAI OpCo, LLC
[2] EU Privacy Policy, OpenAI OpCo, LLC – 10. Data transfers - Adequency decision to Article 45
[3] Product compliance features, OpenAI OpCo, LLC – SOC2, type 2
[4] EU Privacy Policy, OpenAI OpCo, LLC – 10. Data transfers
[5] Coordinated vulnerability disclosure policy, OpenAI OpCo, LLC – Bug bounty

and appropriate organizational and technical security measures to protect Customer Data. These measures are described in Exhibit B of the Data Processing Addendum and include corporate identity, authentication, and authorization controls, customer identity controls, cloud infrastructure and network security, system and workstation control, data access control, disclosure control, availability control, segregation control, risk management, personnel vetting and training, physical access control, third-party risk management, and security incident response[6].

c) **Ethical considerations:** users should avoid sharing content that violates the Content Policy or that may offend others. When content is co-authored with the OpenAI API, the role of AI in formulating the content must be clearly disclosed, and it should not violate OpenAI's Content Policy or Terms of Use[7].

d) **Output generated IP rights:** As between you and OpenAI, and to the extent permitted by applicable law, you (a) retain your ownership rights in Input and (b) own the Output. We hereby assign to you all our right, title, and interest, if any, in and to Output.

4. Data privacy

a) **Data location, collection and processing**: data is stored on OpenAI servers in the USA, primarily based on Microsoft infrastructure, and that data goes outside the EU. The Data Processing Addendum governs OpenAI's processing of Customer Data. OpenAI processes Customer Data as a Data Processor on behalf of the Customer (the Data Controller)[8].

b) **Personal data collection by product**[9]:

(1) Account information: when you create an account with us, we will collect information associated with your account, including your name, contact information, account credentials, date of birth, payment information, and transaction history, (collectively, "Account Information").
(2) User content: we collect Personal Data that you provide in the input to our Services ("Content"), including your prompts and other content you upload, such as files, images, and audio, depending on the features you use.
(3) Communication information: if you communicate with us, such as via email or our pages on social media sites, we may collect Personal Data like your name, contact information, and the contents of the messages you send ("Communication Information").

c) **Model training and evaluation with user data**: free yes, pro versions need to disable it manually. Team and Enterprise have them turned off by default.

d) **Data retention and deletion**:

[6] Data Processing Addendum, OpenAI OpCo, LLC – Exhibit B, Security measures
[7] Ownership of content, OpenAI OpCo LLC
[8] EU Privacy Policy, OpenAI OpCo, LLC – 10. Data transfers
[9] EU Privacy Policy, OpenAI OpCo, LLC – 2. Personal data we collect

(1) OpenAI has specific retention periods for different types of customer data, with API data generally kept for 30 days and ChatGPT Enterprise data retained during the agreement term, unless required otherwise[10].
(2) Upon termination of the data processing agreement, customer data is to be deleted within 30 days, unless legally prohibited[11].
(3) OpenAI also outlines general data retention practices in their privacy policies, stating they keep data only as long as necessary for various legitimate purposes.
(4) Users have the right to request the deletion of their personal data.

5. Risks identification and mitigation
   a) **Operational risks**: misuse with inappropriate content, usage of the product with client's trade secrets, sensitive data / code is used in AI model training, or usage of the data that infringe the copyrights or IP rights of the other entities.
   b) **Human oversight requirements**: **Sharing & Publication Policy requires manual review of AI-generated content before sharing**[12] [13]. For applications built with the OpenAI API Platform, the developer is responsible for designing and implementing how users interact with the technology. This implies a need for human oversight in the deployment and use of the AI assistant.
6. **Potential harm and unintended consequences**: The Usage Policies outline various prohibited uses that could lead to harm, such as compromising privacy, engaging in illegal activities, generating misinformation, and creating inappropriate content. Mitigation involves user training on responsible use, implementation of OpenAI's safeguards, and monitoring for policy violations. OpenAI's indemnification obligations to API customers under the Agreement include any third party claim that Customer's use or distribution of Output infringes a third party's intellectual property right.[14]
7. Usage and monitoring
   a) **Monitoring mechanisms**: OpenAI mentions using a combination of **automated systems, human review, and user reports** to find and assess violations of their policies[15]. Only Enterprise version provide option to monitor it[16].
   b) **User feedback collection**: OpenAI encourages responsible vulnerability research and disclosure through their **Bug Bounty Program**. The Sharing & Publication Policy also mentions using reporting tools within Playground or emailing OpenAI for specific completions[17].
8. Summary and decision

[10] Data Processing Addendum, OpenAI OpCo, LLC – 8. Term, Data Return and Deletion
[11] Data Processing Addendum, OpenAI OpCo, LLC – 8. Term, Data Return and Deletion
[12] Sharing Publication Policy, OpenAI OpCo, LLC – Social media, livestreaming, and demonstrations
[13] Terms of Use, OpenAI OpCo, LLC – Content
[14] Service Terms - https://openai.com/policies/service-terms/
[15] Usage Policies, OpenAI OpCo, LLC – Building with ChatGPT
[16] Introducing ChatGPT enterpise, OpenAI OpCo, LLC – Features for large scale deployments
[17] Usage Policies, OpenAI OpCo, LLC – Social Media, Livestreaming, and demonstrations

a) Risk level determination: **Significant**

b) Approval from Quality leader and IT leader: **not approved**

c) Reviews recommendations: due to easiness of the product accessibility and likely risk of information breached company decided that will disallow usage of ChatGPT. Alternative product for daily work is Microsoft Copilot which is integrated into existing digital workspace ecosystem.