staffino®

AI Feedback Processing Security

1. **Which version of AI Staffino is using?**

   Azure OpenAI, using cutting-edge AI models like GPT-4o, DALL·E, and the o1 series to create custom AI-powered experiences.

2. **What data is being sent to AI?**

   Staffino sends only verbatim (open text answers) data for AI processing and doesn't share any personal data about the customer or the company.

3. **What if personal data or sensitive information will be shared in open question?**

   Staffino AI engine can be trained to **recognize sensitive** (sickness, disablement, psychological issues topics etc.) and **personal data**. In this case **no response will be generated and feedback will be directed to a human agent.**

4. **How is customer data protected from unauthorized access?**

   Customer data is stored in **Staffino's AWS cloud services** (database) and is protected through **secured API communication** between Staffino and Azure OpenAI using API keys. Additionally, only **registered and dedicated users with granted permissions** can access the setup console, and **all events are monitored via an audit log** to track unauthorized access attempts.

5. **Does the AI comply with GDPR, CCPA, or other data privacy regulations?**

   Yes, the AI solution complies with data privacy regulations such as **GDPR and CCPA**, as Azure OpenAI does not receive any customer or employee data—only the **text responses from feedbacks** are sent for evaluation. Additionally, Microsoft provides **transparency notes** and adheres to strict **privacy policies**.

6. **Is customer data encrypted during storage and transmission?**

   Yes, **data storage and transmission** are protected. Customer data is stored securely in **Staffino's AWS cloud services**, and communication between **Staffino and Azure OpenAI is encrypted and secured** using API key authentication.

7. **Who has access to AI-generated responses and stored conversations?**

   Only **registered and authorised users** have access to the setup console and AI-generated responses. All events are logged via **AWS audit monitoring**, ensuring accountability and restricted access. Actual list of Staffino Sub Processors is available on https://staffino.com/legal/sub-processors/ (only selected sub-processors have access to feedback verbatims and AI responses based on their role)

8. **How long is customer feedback data retained, and can it be deleted?**

   Customer feedback data is **stored in Staffino's AWS database**. The exact retention period depends on contract duration and conditions agreed between client and Staffino, but since Azure OpenAI **does not store logs or request history**, there is no risk of long-term data retention on Microsoft's side.
   Deletion policies are managed within **Staffino's AWS cloud infrastructure** and are described in Service Agreement Between client and Staffino.

9. **Can we restrict AI access to specific customer data fields?**

   Yes, AI access is **already restricted** because only **text responses** from feedback are sent for evaluation—**no customer or employee data is shared** with Azure OpenAI. This ensures that sensitive customer information remains protected.

10. **How does the AI prevent malicious inputs, such as phishing attempts?**

    The AI processes **only text feedback responses**, which minimizes the risk of handling sensitive customer information. Additionally, Azure OpenAI's built-in **moderation and filtering** mechanisms can help detect and prevent **malicious inputs** such as phishing attempts or harmful content.

11. **Are AI-generated responses monitored for compliance and accuracy?**

    Staffino admins have access to the **setup console**, where AI-generated evaluations can be monitored. Additionally, **audit logs track all events** to ensure compliance. Microsoft's **transparency policies and OpenAI API documentation** also outline security and compliance measures.

12. **What measures are in place to prevent AI from exposing sensitive information?**

    The AI does not receive any **customer or employee data**—it only evaluates **text feedback responses**. Additionally, Azure OpenAI does **not store any request history or logs**, ensuring that sensitive information is not retained or exposed. Additionally AI can be trained to tag feedbacks, where sensitive or personal information is shared by customer and keep it for human processing.

13. **Has the AI system been penetration tested for security vulnerabilities?**

    Microsoft Azure OpenAI services follow **strict security protocols** and undergo **regular security assessments**. Additionally, Staffino's **API-based integration** with Azure OpenAI ensures **secure communication** with controlled access to data.