FMG Platform AI Policy & Ethos

At FMG, we recognize the transformative potential of Artificial Intelligence (AI) in the financial services industry. Our commitment is to harness AI responsibly, prioritizing the security and privacy of our customers' data while enhancing their experience with innovative tools. We carefully select and integrate AI technologies that align with our high standards for data protection.

I. Current AI-Powered Capabilities

Our products currently incorporate AI to deliver the following key features:

A. Muse: creative content generation tools.

B. Overwatch: tools to streamline compliance without replacing the compliance office and workflow.

C. Sidekick: support and product tools to get product assistance.

II. Principles Guiding Our AI Selection and Integration

FMG does not publish a list of specific LLMs or AI solutions in use. However, FMG uses a robust vendor review process for SOC2 compliance. At the present time, FMG uses only publicly hosted LLMs within its products and services. As with all of our critical vendors, FMG reviews its relationships with AI providers on an annual basis.

When evaluating and integrating AI technologies into our products, FMG adheres to stringent criteria:

A. **Security:** We only utilize AI solutions with robust security protocols to protect customer data.

B. **Data Privacy:** We carefully assess the data privacy practices of potential AI partners to ensure alignment with our commitment to safeguarding customer information.

C. **Reliability and Performance:** We select AI technologies that demonstrate a high degree of reliability and deliver effective performance for their intended purpose.

D. **Reputable Providers:** We partner exclusively with reputable AI providers based in the United States to ensure contracts are governed by U.S. law and are easily enforceable, minimizing legal risk.

E. **Data Usage Restrictions:** Our agreements with all AI providers explicitly prohibit them from using any data we provide for training their future public AI models.

F. **Commercial Protections:** We utilize only commercial terms and protections.

G. **Copyright Indemnification:** We ensure that all generative AI models we use provide copyright indemnification.

III. Data Handling and Training of AI Features

The AI features within FMG products are designed to operate *without* training on customer data.

A. Our AI products and features function without unnecessary ingestion of customer contact data.

B. FMG does not currently train custom models or fine-tune models. If we change our approach, we will take proper steps to ensure anonymization and update our policy.

C. To evaluate and ensure the quality of our AI tools, we leverage both synthetic and proprietary datasets to build internal evaluation frameworks.

D. Currently, the primary interaction with customer-provided data involves the processing of draft marketing messages by features like Muse.

E. FMG logs all requests made to our AI tools. This data helps us understand user behavior, identify potential misuse, and inform ongoing product improvements.

IV. Data Security and Location for AI Processing

FMG prioritizes the security of data processed by our AI features:

A. All AI servers utilized by our products are hosted within the United States with reputable commercial entities.

B. Our model providers are contractually obligated not to train new models on any data we provide.

C. Our agreements with model providers stipulate that they do not retain our data longer than necessary for legal compliance.

D. Our overall vendor management, including AI partners, is subject to annual review as part of our SOC 2 compliance.

V. Compliance with Data Privacy Regulations

FMG is committed to adhering to relevant data privacy regulations in the integration and operation of our AI features.

A. FMG's AI features are not designed to process or store any PII, PHI, confidential, or non-public customer information. Our AI Policy Steering Committee evaluates all product changes quarterly to ensure compliance.

VI. Accuracy and Responsible Use of AI Outputs

While our AI features are designed to be helpful, FMG emphasizes the importance of human oversight:

A. Content generated by our AI tools is intended to be reviewed and approved by an advisor before utilization. In most regulated contexts, this content will also flow through established compliance workflows.

B. We continuously strive to improve the accuracy and quality of our AI outputs through internal evaluations and user feedback mechanisms.

C. All our AI tools include feedback mechanisms to enable users to report improvements and contribute to our ongoing evaluation efforts.

D. We are transparent with our users that, like any AI tool, our features can occasionally make errant assumptions or other mistakes. We advise users to exercise caution and review outputs accordingly before utilizing those outcomes.

VII. Incident Response for AI-Related Issues

FMG maintains a comprehensive Incident Response plan to address any security incidents, regardless of whether AI components are involved. This plan is periodically reviewed and updated as needed.

VIII. Access Control to AI Infrastructure

Access to the underlying AI infrastructure supporting our product features is managed with a strong emphasis on security:

A. Our approach aligns with industry standards, emphasizing the principle of least privilege and, where feasible, the separation of duties.

B. Infrastructure access is granted to experienced senior resources who undergo management selection and approval.

C. Access to this infrastructure is reviewed on a quarterly basis.

IX. Contractual Assurances

FMG's commitments regarding data security, confidentiality, and integrity apply uniformly to all data handled by our products and services, including that processed by AI features. For specific details, please refer to our Privacy Policy, the Security page on our website, and documents available through our Trust Center.

X. Security Assessments

FMG employs a comprehensive suite of security testing methodologies for all product features, including those powered by AI. This includes manual code review, static code analysis (SAST), dynamic security testing (DAST), and regular penetration testing conducted by experienced third-party experts.

XI. Monitoring and Addressing AI Issues

FMG is proactive in monitoring and addressing potential issues with our AI features:

A. We deploy various tools and processes to ensure the safety and quality of AI outputs within our products.

B. All AI-powered features undergo the same rigorous quality assurance processes as non-AI code, including evaluations for accuracy, hallucinations, biases, and safety.

C. User feedback mechanisms are integrated into all our AI tools to facilitate continuous improvement based on real-world usage.

XII. Explainability and Transparency

Currently, as FMG leverages existing AI models rather than developing our own, we do not directly utilize model explainability tools. However, we are closely monitoring the evolution of these tools and intend to adopt them as they become more accessible and mature.

XIII. Customer Control and Opt-Out Options for AI Features

FMG is committed to providing our customers with control over their experience with AI features. In many cases, enterprise clients have the option to opt out of specific AI-powered features within our products.