Domo.AI Security and Privacy

Frequently Asked Questions

Scope

This document refers to Domo.AI only. Specifically, the features included are:

- AI Chat (using DomoGPT)
- Beast-mode assistant
- AI Services from Apps/Bricks/Workflows
- AI Model Management

Any features or functions outside this list are not covered by this policy.

What data is collected and how is it used?

At Domo, transparency and user control are core principles that guide our approach to responsible AI development. We are committed to being fully transparent about the data we collect and how it is used to provide the various Domo.AI functionalities to our customers. Domo.AI will only work with the data you ingest into the Domo platform. Currently, we do not use customer data to train internal Domo AI models (DomoGPT) or any third-party models that we utilize in our AI offerings.

We will provide you with clear and detailed information about the specific data elements we collect, the sources of that data, and how it is being used. This includes disclosing any instances where we may share data with external third parties.

How is the data protected?

Protecting the privacy and security of your data is of the utmost importance to us. We have implemented robust data governance and security measures, including encryption, access controls, regular audits, and continuous monitoring, to safeguard your information. We are compliant with all applicable data protection regulations such as GDPR, CCPA, etc., and your data is handled with the highest standards of care as per the leading security frameworks and standards such as SOC 2 Type II, ISO 27001, ISO 27018, HITRUST, NIST CSF, and HIPAA. This data protection is fully extended to Domo.AI's capabilities.

Is customer data used to train AI models?

No, our current AI offerings do not use customer data to train AI models.

Is customer data sent to external third parties outside of Domo?

Currently, our default AI offerings use Domo hosted Large Language Model called DomoGPT. With DomoGPT, customer data remains within Domo's secure private cloud within AWS infrastructure (using Amazon Bedrock) and all of Domo's data protection controls are fully extended to safeguard customer data within this private cloud. AWS does not log or store customer prompts and completions, and model providers (eg. Anthropic) do not have access to customer prompts and completions. All requests to DomoGPT stay within Domo private cloud and do not communicate with or traverse any public, external, or non-Domo hosted endpoints.

In cases where DomoGPT is not currently available, eg. Domo's Azure infrastructure, our default offerings use OpenAI's API platform. In addition, under AI Model Management, Domo.AI supports external models from leading tools such as OpenAI, Hugging Face, Gemini, Databricks, Amazon Bedrock, etc. If using DomoGPT, no customer data is sent to any external third parties. For AI Chat and Page Generation features, if DomoGPT is disabled, customer data is sent to OpenAI using their API platform. Customers have the ability to disable Domo provided OpenAI models within Admin AI Service settings. OpenAI's API platform does not train on any of our customer data or business data as per their enterprise agreement with Domo. It has been audited and certified for SOC 2 Type 2 and HIPAA compliance, and API inputs and outputs are retained for up to 30 days to provide the services and to identify abuse, before they are deleted.

Can customers control or limit the use of their data?

Customers have full control over their data and can specify how it is used within our platform. We provide comprehensive privacy settings that allow customers to customize their data preferences and opt-out of certain data processing activities if desired.

What happens to the data when it is no longer needed?

We have clear data retention and deletion policies in place to ensure that your data is only kept for as long as it is necessary for the provision of our AI offerings. Once your data is no longer needed, we will securely delete it in accordance with industry best practices and regulatory requirements. You can request the deletion of your data at any time.

How are security considerations integrated into the AI development process?

We follow a Secure Development Lifecycle (SDLC) that includes thorough threat modeling, secure coding practices, and rigorous testing to identify and address vulnerabilities. Our approach aligns with the OWASP Top 10 for Large Language Model (LLM) Applications, ensuring measures are in place to mitigate risks like insecure output handling, model poisoning, and supply chain vulnerabilities. Data governance is central to our practices, with stringent policies on data anonymization, encryption, and compliance with regulations such as GDPR and CCPA. Transparency and explainability are key features of our AI models, providing insights into decision-making processes. With these measures in place, we are dedicated to building AI solutions that are not only innovative but also secure, transparent, and privacy focused.

What are Domo's data privacy policies and compliance with regulations?

Our data privacy policies are designed to meet or exceed the requirements of all relevant data protection regulations, such as the GDPR and CCPA. We undergo regular audits and assessments to ensure our compliance, and we are committed to being transparent about our data practices. In the event of a data breach or security incident, we have robust incident response and notification procedures in place to protect your interests.

What are the risks of data misuse or non-compliance with privacy regulations?

We understand the serious consequences that can arise from data misuse or non-compliance with privacy regulations, including legal liabilities, reputational damage, and financial penalties. That is why we have implemented comprehensive measures to mitigate these risks and protect your data. We are committed to the ethical and responsible use of AI technology, and we will always be upfront about any potential risks or issues that may arise.

How does Domo minimize data privacy risks when using third-party AI services?

We have established a Responsible AI (RAI) program that encompasses robust data management practices, such as anonymization, encryption, and consent management. We also engage in regular collaboration and transparency with our customers to ensure that our AI services are aligned with customers' specific data privacy and security requirements. By working closely with our customers, we can help navigate the complexities of third-party AI usage and ensure that customer data is protected at every stage.

Does Domo document what types of output and or recommendations each model makes? Is that documentation securely stored?

Domo's AI Chat does document the steps it takes to come up with its response in the UI, typically the dataset and SQL used as a basis for its response. All documentation related to the output of the models are securely stored within Domo Production infrastructure. We can highlight the SOC 2 report which lists several controls which we have implemented to safeguard customer data and our infrastructure/application.

What controls does Domo provide to its customers to prevent insider misuse of the AI functionality?

Role based access controls (RBAC) including custom roles, grants, cryptographic controls to safeguard data at rest and transit, and detailed activity logs which can also be exported to the customers SIEM for further detailed analysis, monitoring, and alerting.

Does Domo have an AI/ML incident response plan? Is it a separate document or combined with another plan?

Yes, it is included as part of Domo's formal IRP.

How do you quantify sociological bias in Domo's AI/ML training data and model predictions? Do you maintain current awareness of how each model affects different demographic customer segments?

We perform internal testing before we onboard new models on DomoGPT and may periodically assess existing models for safety, security, and appropriateness. We do not disclose our testing practices currently.

What AI best practices does Domo utilize when implementing AI/ML?

Domo adheres to key Responsible AI principles such as reliability, safety, accountability, and transparency. We also empower developers with tools and resources to identify, debug, and mitigate undesirable AI behaviors. In addition, we have implemented robust access controls, logging, and monitoring to prevent unauthorized access or misuse of AI systems. Lastly, we have implemented clear policies and processes for investigating and addressing any violations or misuse of AI.

Have any independent third parties or other external experts (legal, security, or others) been involved in your company's procedures to address the known liabilities of AI/ML?

Yes, our SDLC process, which includes development practices for AI, have been audited by external third parties as part of our SOC 2, ISO 27001, ISO 27018, and HITRUST certifications.