Collective Data AI Trust FAQs

Last Update: January 2025
Collective Data leverages artificial intelligence (AI) to enhance its platform capabilities and provide users with advanced tools for data management, analysis, and process automation. By integrating AI technology, we aim to streamline operations, offer predictive insights, and enhance decision-making processes for our customers.

We prioritize privacy and security in the development of our AI products, and this FAQ addresses data security, compliance, governance, and user controls. Our goal is to ensure transparency and build confidence in our trust posture.

For more details on our security and compliance initiatives, please email security@collectivedata.com or refer to our detailed compliance documents.

Security & Governance

How does Collective Data protect and secure customer data within AI models and products?
At Collective Data, security is our highest priority. We implement robust technical and organizational controls to protect customer data, including:

- Encryption of data in transit and at rest following our **Cryptography Policy**.
- Role-based access control (RBAC) for systems and data in alignment with our **Access Management Policy**.
- Comprehensive vulnerability assessments per our **Vulnerability Management Policy**.
- All AI products are developed to ensure compliance with security frameworks such as NIST 800-53 and ISO 27001. Sensitive data is securely stored and handled as per our **Data Management Policy** to prevent unauthorized access or disclosure.

How does Collective Data ensure AI usage complies with laws and industry standards?

Our compliance program includes collaboration between legal, product, and engineering teams to align our AI products with regulatory and industry requirements. Our SOC 2

compliance is grounded in NIST 800-53 and ISO 27001 frameworks, ensuring our practices meet stringent security and data protection standards.

Does Collective Data use customer data to train its AI models?

No, Collective Data does not use customer data to train AI models under any circumstances. Customer data is isolated and remains within their application instance. Customers may opt out of using AI features entirely by contacting their support team at clientsuccess@collectivedata.com or the security and compliance team at security@collectivedata.com.

How does Collective Data moderate AI outputs?

We are committed to ensuring that our AI-generated content aligns with ethical guidelines. AI products undergo rigorous testing to minimize the risk of inappropriate or harmful outputs. Any anomalies are reported and mitigated through our **Incident Response Policy**.

Is customer data shared with third-party AI vendors?

Collective Data does not share customer data with third-party vendors to train AI models. AI functionality operates entirely within our secure systems, ensuring that customer data remains private and protected at all times.

What oversight exists for AI tool development at Collective Data?

Collective Data has established an "AI Committee" responsible for overseeing the development and deployment of all AI tools. This committee includes representatives from engineering, security, compliance, and product teams. The AI Committee ensures that:

- All AI tools are developed with security, ethical, and legal compliance in mind.
- Regular reviews are conducted to identify potential risks and improvements.
- Policies and standards for AI development align with Collective Data’s broader compliance framework.

Customer Control & Choices

What controls do customers have over using Collective Data AI products?

Customers have the option to disable AI features entirely within their application. To make this change, please contact our support team at clientsuccess@collectivedata.com or the security and compliance team at security@collectivedata.com.

Can customers review or delete their data used in AI products?

Yes. Collective Data empowers customers to manage their data as per the **Data Management Policy**. Customers can review, download, or request deletion of their data directly through the platform or by contacting our support team.

Transparency & Compliance

What certifications or audits does Collective Data adhere to for AI products?

Our AI products are developed and maintained in accordance with:

- SOC 2 Type 2 certification based on NIST 800-53 and ISO 27001 frameworks.
- Regular third-party audits as part of our vendor management and risk assessment programs.

Does Collective Data's AI automatically prevent copyright infringement?

While our AI products are designed to minimize risks such as plagiarism or inappropriate content, users are responsible for ensuring compliance with copyright laws when using AI-generated outputs.

Data Usage

How does Collective Data handle sensitive data?

Sensitive customer data is not used in AI model training or shared with third-party vendors. All customer data is encrypted and securely stored in compliance with our **Data**

Management Policy. Customers may opt out of using AI features entirely by contacting clientsuccess@collectivedata.com or the security and compliance team at security@collectivedata.com.

Can customers use Collective Data AI outputs commercially?

AI-generated outputs are intended for use exclusively within the Collective Data application. They are not designed or licensed for commercial use outside the platform.

How is Collective Data AI tested and monitored for quality assurance?

Our **Quality Assurance and Change Management Process** ensures that AI products undergo rigorous testing before release. Performance, security, and ethical considerations are monitored continuously through automated systems and regular reviews.

Resources
For more details, request our:

- Contact our security and compliance team at security@collectivedata.com.