# Data Security and Processing Addendum

For ThreatGEN AutoTableTop™ EULA

This *Data Security and Processing Addendum* ("**Addendum**") is an integral part of the End User License Agreement ("**EULA**") for ThreatGEN's AutoTableTop™ SaaS product. It outlines ThreatGEN's commitment to data security, privacy, and compliance with applicable laws, including internal SOC 2 standards. This Addendum also describes how customer data is processed during the use of AutoTableTop™.

1) SOC 2 Management Assertion

   ThreatGEN has conducted an internal audit of its AutoTableTop™ system to ensure compliance with the Trust Services Criteria (TSC) for SOC 2 standards. While we have not undergone an independent SOC 2 audit, we assert that our system has been designed and operated in alignment with SOC 2 principles, specifically regarding security, availability, processing integrity, confidentiality, and privacy.

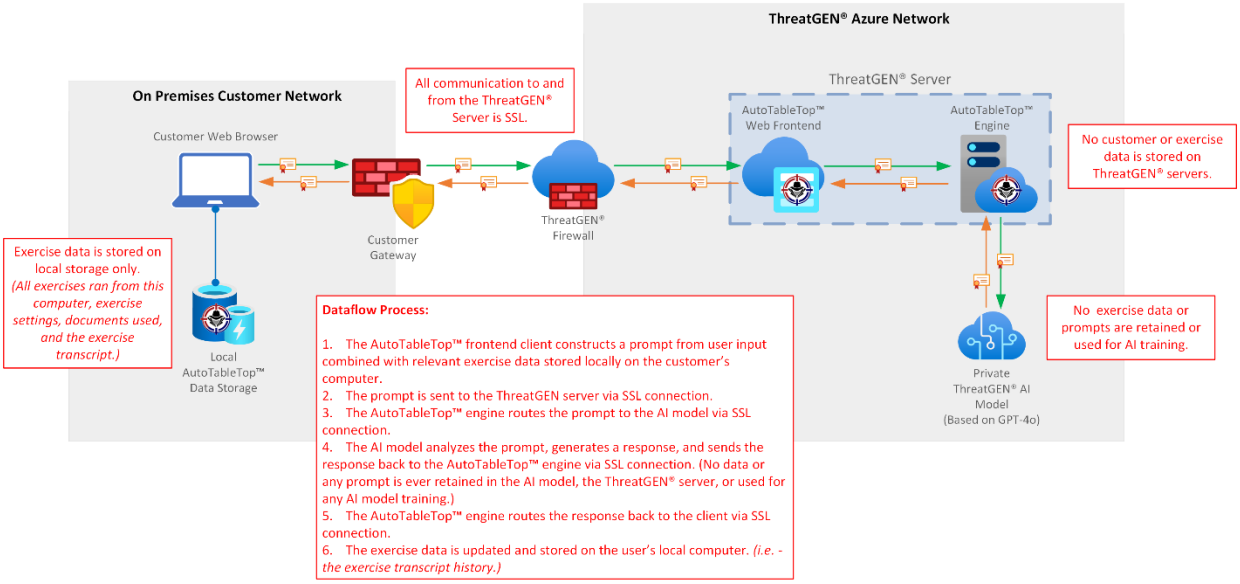
   Key Assertions:

   - Security: Our controls are designed to prevent unauthorized access and protect data integrity. We utilize Microsoft Azure hosting services with integrated Azure Web Application Firewall (WAF) to defend against common web vulnerabilities.
   - Availability: We maintain high availability of our services through robust infrastructure support provided by Azure.
   - Processing Integrity: Our processes ensure accurate and complete data processing using advanced AI models in a secure sandbox environment.
   - Confidentiality: Sensitive information is protected from unauthorized disclosure via real-time monitoring and logging through Azure WAF.
   - Privacy: We handle personal information in compliance with applicable privacy laws and regulations.

   **A copy of our internal SOC 2 Management Assertion document is available upon request.**

2) Data Flow Process

   The following outlines the secure data flow within the ThreatGEN AutoTableTop™ system:




Data Flow Diagram Overview:

The diagram above illustrates how customer data flows between the customer's local environment and ThreatGEN's servers during tabletop exercises.

Key Points:

- Local Data Storage: All exercise-related data (e.g., settings, documents used, transcripts) is stored locally on the customer's workstation. No exercise data is stored on ThreatGEN's servers.
- SSL Encryption: All communication between the customer's network and ThreatGEN's servers is encrypted using SSL to ensure secure transmission.

Data Flow Process:

- The AutoTableTop™ frontend client constructs a prompt from user input combined with relevant exercise data stored locally on the customer's computer.
- The prompt is sent securely to ThreatGEN's server via SSL.
- The AutoTableTop™ engine routes the prompt to our private AI model for analysis via SSL.
- The AI model generates a response based on the prompt and sends it back to the AutoTableTop™ engine via SSL.
- The response is transmitted back to the customer's local computer via SSL.
- The exercise transcript is updated locally on the customer's workstation.

**Important Note**: No customer or exercise data is retained by ThreatGEN servers or used for AI training purposes.

3) Data Processing Terms

Types of Data Processed:

- Personal Information: We collect minimal personal information required for user registration (first name, last name, email address). This information is stored securely in accordance with our Privacy Policy included within our EULA.
- Exercise Data: All exercise-related data (e.g., settings, documents used, transcripts) is processed locally on the customer's workstation and not retained by ThreatGEN.

Purpose of Processing:

The primary purpose of processing personal information and exercise data is to facilitate tabletop exercises using AutoTableTop™. Personal information may also be used for account management and support purposes.

Customer Responsibilities:

Customers are responsible for securing their own network environments, including ensuring that local storage where exercise data resides is adequately protected from unauthorized access or breaches.

4) Security Measures

ThreatGEN employs industry-standard security measures to ensure that all interactions between customers and our systems are secure:

- SSL Encryption: All communication between customer networks and ThreatGEN servers is encrypted using SSL protocols.
- Local Data Storage: Exercise data remains on local storage only; no exercise-related files are stored on ThreatGEN servers.
- No Data Retention: No prompts or exercise data are retained by ThreatGEN or used for AI training purposes.

Our system architecture ensures that sensitive information remains under the control of the customer at all times.

5) Data Subject Rights

Customers have full control over their exercise data stored locally on their workstations. Personal information stored by ThreatGEN can be accessed or deleted upon request in accordance with applicable privacy laws.

6) Breach Notification Procedures

In the event of a security breach affecting personal information or sensitive exercise data processed by ThreatGEN, we will notify affected customers without undue delay after becoming aware of such a breach. Notifications will include details of the breach, potential impacts, and recommended actions for mitigation.

7) Subprocessors

ThreatGEN may engage subprocessors for certain functions related to service delivery (e.g., hosting services through Microsoft Azure). Any subprocessors used will be bound by appropriate contractual obligations regarding security and confidentiality in line with this Addendum.

8) International Data Transfers

All personal information processed by ThreatGEN remains within jurisdictions that comply with applicable privacy regulations (e.g., GDPR). Any international transfers of personal information will be conducted in accordance with legal requirements.

9) Audit Rights

Customers may request documentation related to our internal SOC 2 assertion or engage in discussions regarding our security practices as part of their due diligence process.

10) Termination and Data Deletion

Upon termination of services or at your request, all personal information stored by ThreatGEN will be deleted in accordance with applicable legal requirements. Exercise data remains under your control as it resides locally on your workstations.

11) Liability and Indemnification

ThreatGEN’s liability related to data processing under this Addendum is limited as outlined in the EULA's "*Limitation of Liability*" section. Customers agree to indemnify ThreatGEN against any claims arising from their failure to comply with their own security responsibilities as outlined in this Addendum.