Schedule A

Data Processing Profile

Radware's Agentic AI Service

This Data Processing Profile is supplemental to a Data Processing Agreement ("**DPA**") between Radware Ltd./Inc. ("**Radware**" or "**Processor**") and the entity that has executed or accepted the DPA ("**Customer**" or "**Controller**"). This Data Processing Profile describes the processing of personal data (or personally identifiable information) by Radware in connection with Radware's **Cloud Web Application Firewall (CWAF) Service** (the "**Service**"). Capitalized terms used in this Data Processing Profile but not defined herein shall have the meanings ascribed to them in the DPA.

Service Overview

Radware's Agentic AI Service protects applications and application programming interfaces ("APIs") (the "**Protected Assets**") against Agentic and LLM attacks.

The Service features a Customer Service Portal, which provides visibility into the logs and functions of the Service. Configuration options, such as adding agents and setting Agents platform, may be defined and managed using the Radware Unified Cloud Service Portal ("Service Portal").

Customer Selectable Features

Agent Inventory
The service provides full visibility into AI agent interactions, automations, and data connectors, breaking down each agent's activity into step-by-step insights that reveal what data is accessed, where it's sent, and which tools or connectors are involved-creating a forensic trail to identify potential leakage paths early. It continuously scans and identifies agents across the environment, maps their relationships within applications to visualize dependencies and traffic flow, monitors long-term behavioral patterns to detect anomalies and usage trends, and offers rich metadata on agent, usage, and associated tools.

Agent Behavioral Protection The service provides real-time enforcement of agent behavior, ensuring AI agents operate within intended boundaries during execution. If an agent attempts unauthorized or unintended action, such as accessing sensitive data or triggering a workflow without proper context the system immediately blocks the activity and generates a detailed report. Runtime monitoring continuously observes agent actions to detect and mitigate malicious or anomalous behavior, offering real-time protection across the full spectrum of agentic risks. These include agent behavior hijack, which protects against manipulation of an agent's goals for an attacker's benefit; tool misuse and exploitation, where agents are tricked into using their tools in harmful or unintended ways; memory and context poisoning, which corrupts agent memory or context to distort reasoning and decision-making; rogue agents, referring

to malicious or compromised external agents acting autonomously to deceive or disrupt protected agent behavior; and secure access, which restricts actions to authorized agents, controls tool activation based on user permissions, and enhances overall system security and compliance.

Allow/Block tool control To prevent unauthorized data movement and ensure operational integrity, the service enforces granular policies across connectors, domains, and endpoints. Security teams can define which tools and destinations are permitted for agent interactions, effectively creating guardrails that restrict agents from sending data to unapproved locations or integrating with risky third-party services. This control mechanism helps maintain compliance with internal policies and external regulations, while also reducing the attack surface by limiting exposure to untrusted environments. By tightly managing agent access to external systems, organizations can ensure that AI-driven workflows remain secure and predictable.

AI Posture This capability delivers continuous assessment of the security posture across all AI agents and their associated tools by identifying targeted data exposures, multi-agent risk flows, and behavioral anomalies. Risks are scored in based on severity to help prioritize remediation. To prevent future violations, the system recommends applying targeted controls, refining agent permissions, and tightening policy enforcement based on observed risk patterns

Purpose of the Processing

Processing is performed to protect the Customer's Applications from Agent and LLM attacks, such as the "OWASP Top 10 LLM" and "OWASP Top 10 Agentic AI".

Processing of Data in Transit

The Service processes all traffic, including legitimate and malicious, flowing to the Customer's Protected Agentic Environment and detects communications between agents and the LLM provider.
Data in transit may include all categories of Personal Data contained in the Customer's Agent data stream.
Processing activities consist of decrypting the traffic, performing security inspection.

Data at Rest

Repository	Data Description		Retention Period
Customer Portal Database	Security event metadata for the purpose of presenting status and statistics to the Customer through the Service portal, managing the Service. The following security alerts information is stored: Attacker/malicious actor information: - Source Attack/malicious activity information: - OWASP category - Security Module - Violation type - Raw Request		1 months
Account Information and configuration data	Data related to the Customer's account in the Service Portal. Subscription: - Account name - Subscription period - Service plan - Contact information - Users		Stored as long as the Customer account is active. Deleted once the customer stops using the service.
Logs Feature	Agent-to-LLM communication The following information is stored: - Agent Request - LLM Response		1 month
	AWS Bedrock	- Content Data - Conversation History - Model Configuration - Tool Definitions & Usage - Identity & Access - Session & Interaction Metadata - Platform & API Metadata - Usage & Billing Metrics - Protection & Safety	
	Copilot Studio	- Content Data - Session & Interaction Metadata - Identity & Access - Platform & API Metadata - Content Delivery & Rendering - Protection & Safety	

	M365 Copilot	- Content Data - Content Delivery & Rendering - Session & Interaction Metadata - Identity & Access - Platform & API Metadata - Protection & Safety	
	Azure AI Foundry	- Content Data - Conversation History - Model Configuration - Tool Definitions & Usage - Identity & Access - Session & Interaction Metadata - Usage & Billing Metrics - Protection & Safety	
	Home grown	- Content Data - Model Configuration - Tool Definitions & Usage - Identity & Access - Session & Interaction Metadata - Platform & API Metadata - Usage & Billing Metrics - Protection & Safety	
Behavior Agent Protection	Agent-to-LLM communication The following information is stored: - Agent Request - LLM Response		Data is only processed and not stored

Data Subjects

Natural Persons include the users of the Customer's Protected Assets and the Customer's employees or agents who administer the Service.

Duration of the Processing

The duration of the processing is determined by the Principal Agreement or until deletion of all Customer's Personal Data in accordance with the DPA and the "Retention Period" set forth in the table above.

Technical and Emergency Support

Technical and Emergency Support is provided to Radware customers according to the agreed Service Level Agreement (SLA).

Industry Standard Certificates

Radware's Agentic AI complies with the following standards for cybersecurity and privacy:

- *ISO 22301* Business Continuity Management System
- *ISO 27001* *Information Security Management System*
- *ISO 27032* *Security Techniques -- Guidelines for Cybersecurity*
- *ISO 27017* *Information Security for Cloud Services*
- *ISO 27018* *Information Security Protection of Personally identifiable information (PII) in public clouds*
- *ISO 27701* *Data Privacy Management System*
- *ISO 42001* *AI Management System conducted*
- *HIPAA* *Health Insurance Portability and Accountability Act*

Radware is compliant with *ISO 28000 Specification for Security Management Systems for the Supply Chain.*

Compliance with these standards is audited annually by third party auditors.

Customers may find Radware's latest cybersecurity and privacy certifications and attestations at https://www.radware.com/newsroom/certificationsindustry/

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 6971917, Israel

Tel: 972 3 766 8666