SPARTA SERVICES

Managed Intelligence Provider

Data Processing Agreement

Effective Date	Document Version
July 24, 2026	Version 1.0.0

This Data Processing Agreement supersedes and replaces all prior versions.

INTRODUCTION

This Data Processing Agreement (**"Agreement" or "DPA"**) is entered into between **Sparta Services LLC**, a Washington limited liability company and Microsoft Solutions Partner (sometimes referred to as "Sparta," "Provider," "we," "us," or "our"), and the client identified in the applicable Order or Master Services Agreement (sometimes referred to as "Client," "you," or "your").

This DPA, together with the Order, Master Services Agreement ("MSA"), Schedule of Services, and any relevant Service Attachments, forms part of the Agreement between the parties governing the processing of personal and regulated data in connection with Sparta's managed intelligence, advisory, solution development, and managed service offerings.

The parties agree as follows:

1. Health Insurance Portability and Accountability Act - HIPAA Data Processing

This Section documents the safeguards imposed upon the parties to protect health information subject to the Health Insurance Portability and Accountability Act ("HIPAA"). If HIPAA is identified in the applicable Order, and if Sparta is engaged as a "Business Associate" under HIPAA, then this Section applies to Sparta's activities as a Business Associate for each agreement between Sparta or any Sparta Affiliate and Client or any Client Affiliate under which Sparta engages Protected Health Information.

a. Definitions

The following terms used in this Section have the same meanings as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

"Business Associate" has the meaning set forth at 45 CFR 160.103 and, for purposes of this Agreement, refers to Sparta Services LLC.

"Covered Entity" has the meaning set forth at 45 CFR 160.103 and, for purposes of this Agreement, refers to Client.

"HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

b. Obligations of Business Associate

Sparta, as Business Associate, agrees to:

- Not use or disclose Protected Health Information other than as permitted or required by this Agreement or as required by law;

- Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for by this Agreement;
- Report to Covered Entity any use or disclosure of Protected Health Information not provided for by this Agreement, including breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which Sparta becomes aware;
- Ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Sparta agree to the same restrictions, conditions, and requirements that apply to Sparta with respect to such information, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2);
- Make available Protected Health Information in a Designated Record Set to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;
- Make any amendment(s) to Protected Health Information in a Designated Record Set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526;
- Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy obligations under 45 CFR 164.528;
- Comply with the requirements of Subpart E of 45 CFR Part 164 to the extent Sparta carries out one or more of Covered Entity's obligations under Subpart E; and
- Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules, to the extent required by regulators.

c. Permitted Uses and Disclosures

- Sparta may only use or disclose Protected Health Information as necessary to perform the services set forth in the MSA. Sparta is authorized to de-identify information in accordance with 45 CFR 164.514(a)-(c).
- Sparta may use or disclose Protected Health Information as required by law.
- Sparta agrees to make uses and disclosures and requests for Protected Health Information consistent with Covered Entity's minimum necessary policies and procedures.
- Sparta may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity.
- Sparta may disclose Protected Health Information for the proper management and administration of Sparta or to carry out Sparta's legal responsibilities, provided the disclosures are required by law or Sparta obtains reasonable assurances of confidentiality from the recipient.
- Sparta may provide data aggregation services relating to the health care operations of the Covered Entity.

d. Privacy Practices and Restrictions

- Covered Entity shall notify Sparta of any limitation(s) in the Notice of Privacy Practices under 45 CFR 164.520 that may affect Sparta's use or disclosure of Protected Health Information.
- Covered Entity shall notify Sparta of any changes in, or revocation of, permission by an individual to use or disclose Protected Health Information that may affect Sparta's activities.
- Covered Entity shall notify Sparta of any restriction under 45 CFR 164.522 that may affect Sparta's activities.

e. Permissible Requests

Covered Entity shall not request Sparta to use or disclose Protected Health Information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

2. Gramm-Leach-Bliley Act - GLBA Data Processing

This Section documents the safeguard standards imposed to protect Client financial information subject to the Gramm-Leach-Bliley Act ("GLBA"). If GLBA is identified in the Order, and if Sparta's services constitute processing of financial information governed by GLBA, these provisions apply.

a. Definitions

All capitalized terms not otherwise defined herein have the meanings set forth in Title V of the Gramm-Leach-Bliley Act (P.L. 106-102; 15 U.S.C. §6801 et seq.) and the regulations issued by the applicable Financial Institution's Functional Regulator.

b. Receipt of Information

To perform its duties under the Agreement, Sparta is authorized and permitted to receive, hold, and, to the extent necessary, review Nonpublic Personal Information of Client in order to provide services at Client's direction. Sparta may further use and disclose Nonpublic Personal Information for the proper management and administration of its business.

c. Obligations of Service Provider

Sparta will take reasonable steps to:

- Implement and maintain a written, comprehensive information security program containing administrative, technical, and physical safeguards for the security and protection of Nonpublic Personal Information, including each element set forth in §314.4 of the Gramm-Leach-Bliley Standards for Safeguarding Client Information (16 C.F.R. §314) and applicable Red Flag Rules;
- Ensure the security and confidentiality of Nonpublic Personal Information received from Client;
- Protect against any anticipated threats or hazards to the security or integrity of Nonpublic Personal Information;
- Protect against unauthorized access to or use of such information that could result in harm or inconvenience to Client;
- Ensure the proper disposal of Nonpublic Personal Information as set forth in the MSA or applicable Service Attachments; and
- Notify Client of any loss or breach of the security or confidentiality of Client's Nonpublic Personal Information.

d. Permitted Uses and Disclosures

Sparta may disclose Nonpublic Personal Information received under this Agreement only if disclosure is required by law.

e. Permissible Requests

Client shall not request Sparta to use or disclose Nonpublic Personal Information in any manner that would not be permissible under Title V of the Gramm-Leach-Bliley Act (P.L. 106-102; 15 U.S.C. §6801 et seq.) if done by Client.

3. California Consumer Privacy Act - CCPA Data Processing

This Section documents the safeguard standards imposed to protect Client information subject to the California Consumer Privacy Act ("CCPA"). If CCPA is identified in the Order, and to the extent Sparta's services constitute processing of personal information governed by CCPA, these provisions apply.

a. Definitions

- "CCPA" means the California Consumer Privacy Act of 2018, Cal. Civ. Code §1798.100 et seq., and its implementing regulations.
- "Client Personal Information" means any Client Data processed by Sparta solely on Client's behalf that identifies, relates to, describes, or is reasonably linked to a particular consumer or household, to the extent protected as "personal information" under applicable U.S. Data Protection Laws.
- "U.S. Data Protection Laws" means all applicable laws and regulations of the United States, including the CCPA, governing the processing of personal information.
- "Service Provider" has the meaning set forth in Section 1798.140(v) of the CCPA.

b. Roles

The parties acknowledge and agree that with regard to processing of Client Personal Information performed solely on behalf of Client, Sparta is a Service Provider and receives Client Personal Information pursuant to the business purpose of providing the Services in accordance with the Agreement.

c. No Sale of Client Personal Information

Client and Sparta acknowledge and agree that the transfer of Client Personal Information from Client to Sparta pursuant to the Agreement does not constitute a "sale" of information, and nothing in the Agreement shall be construed as providing for such sale.

d. Limitations on Use and Disclosure

Sparta is prohibited from using or disclosing Client Personal Information for any purpose other than the specific purpose of performing the Services specified in the Agreement, permitted business purposes under applicable law, and as required by law. Sparta certifies that it understands this restriction and will comply with applicable U.S. Data Protection Laws.

e. Data Subject Access Requests

Sparta will reasonably assist Client with data subject access, erasure, or opt-out requests. If Sparta receives any such request from data subjects, authorities, or third parties, it will promptly inform Client and assist Client in developing a response, but will not itself respond other than to confirm receipt and refer the matter to Client, except per Client's written instructions.

f. Data Retention

Sparta will retain only the minimum amount of Client Personal Information essential to fulfill its obligations under the MSA, Service Attachments, and this DPA. Sparta will not keep data longer than necessary without first providing written notice and justification to Client.

4. Washington State My Health MY Data Act & Consumer Protection

This Section documents the safeguard standards imposed to protect Client information under the Washington My Health MY Data Act (ESSB 1155), the Washington Consumer Protection Act (RCW 19.86), and applicable Washington State regulations, including compliance with HB 1155 and SHB 1672 (AI Governance). These provisions apply to all engagements where Sparta processes the personal data or health data of Washington State residents.

a. Consumer Health Data

- Sparta will not collect, use, or disclose consumer health data beyond what is necessary to perform the Services and will not sell consumer health data.
- Sparta will implement and maintain a consumer health data privacy policy as required by the My Health MY Data Act.
- Sparta will honor consumer rights requests (access, deletion, withdrawal of consent) within legally required timeframes and will promptly notify Client of any such requests.
- Sparta will not use geofencing or similar technologies to collect health data in proximity to health care facilities without Client's prior written authorization.

b. AI and Automated Decision-Making (SHB 1672)

- Where Sparta's AI-powered services, including Microsoft Copilot, Azure AI, Copilot Studio, or Sparta-developed AI workflows, process personal data in an automated decision-making capacity, Sparta will maintain an Acceptable Use Policy aligned to Washington State HB 1672 and applicable federal guidance.
- Sparta will provide transparency to Client regarding the use of AI models and automated systems that materially affect the rights or access to services of Washington State consumers.
- Sparta will implement human review mechanisms for high-impact AI decisions as required by applicable law and Client's instructions.

c. General Washington Consumer Protection

- Sparta will not engage in unfair or deceptive acts or practices in connection with the collection, use, or processing of personal data, consistent with RCW 19.86.
- Sparta will maintain data minimization practices and limit personal data collection to what is reasonably necessary for the stated purposes.

5. General Data Protection Regulation for the EU and UK - GDPR

The General Data Protection Regulation ("GDPR") imposes specific obligations on "Processors," "Controllers," and others with regard to vendor relationships. If GDPR is identified in the Order, and to the extent Sparta's services constitute processing of personal information governed by GDPR, these provisions apply. This Section is effective on the date of the applicable Order.

a. Definitions

- "GDPR" means Regulation (EU) 2016/679 and the UK Data Protection Act of 2018, together with applicable implementing legislation issued by supervisory authorities.
- "Controller" has the meaning in GDPR Article 4(7): the entity that determines the purposes and means of processing personal data.
- "Personal Data" has the meaning in GDPR Article 4(1): any information relating to an identified or identifiable natural person.
- "Personal Data Breach" has the meaning in GDPR Article 4(12): a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
- "Processing" has the meaning in GDPR Article 4(2): any operation performed on personal data, whether automated or manual.
- "Processor" has the meaning in GDPR Article 4(8): an entity that processes personal data on behalf of the Controller.
- "Sub-processor" means any processor engaged by Sparta to carry out specific processing activities on behalf of the Controller.

b. Obligations as Processor

Sparta, as Processor, represents that it has implemented appropriate technical and organizational measures such that its processing of Personal Data meets the requirements of GDPR and ensures the protection of data subject rights.

Processing and Security. In accordance with GDPR Article 28(3), Sparta shall:

- Process Personal Data only as needed to provide the Services, in accordance with Client's documented instructions, and as required by applicable law;
- Ensure that persons authorized to process Personal Data have committed to confidentiality or are subject to an appropriate statutory obligation of confidentiality;
- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including pseudonymization, encryption, ongoing availability, resilience, and regular testing of measures;
- Reasonably assist Client in fulfilling its obligation to respond to data subject rights requests;
- Assist Client in complying with obligations regarding Personal Data Breaches (GDPR Articles 33 and 34), data protection impact assessments (GDPR Article 35), and prior consultation (GDPR Article 36);
- At Client's discretion, delete or return all Personal Data after the end of the Services and delete existing copies unless applicable law requires retention;
- Provide Client with all information necessary to demonstrate compliance with GDPR and allow for audits conducted by Client or Client's mandated auditor; and
- Immediately inform Client if, in Sparta's opinion, an instruction infringes GDPR or applicable Member State data protection provisions.

c. Sub-processors

Client provides general authorization for Provider to engage Subprocessors.

Provider shall maintain a list of material Subprocessors and shall provide reasonable notice of material additions or replacements upon request.

Client may object to a new Subprocessor only on documented and reasonable data protection grounds.

If the parties cannot resolve such objection in good faith, Provider may terminate the affected Services without liability.

d. Personal Data Transfers

Sparta shall not Transfer any Personal Data (and shall not permit its Sub-processors to Transfer any Personal Data) without prior consent of Client. Sparta understands that Client must approve adequate protection for the data after Transfer, using standard contractual clauses or another recognized legal basis.

e. Breach Notification

Sparta will promptly and thoroughly investigate all allegations of unauthorized access to, use, or disclosure of Personal Data. Sparta will notify Client without undue delay in the event of any Personal Data Breach, including the details required under GDPR Article 33.

6. New York SHIELD Act

Sparta maintains a comprehensive, written information security program containing administrative, technical, and physical safeguards appropriate to the size, scope, and type of Sparta's business; the resources available; the type of information stored; and the need for security and confidentiality of such information. If SHIELD is identified in the Order and to the extent Sparta's services constitute processing of data under SHIELD, these provisions apply.

Sparta's security program is designed to:

- Protect the confidentiality, integrity, and availability of Customer Data in Sparta's possession or control;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Customer Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard information as set forth in any applicable local, state, or federal regulations.

Without limiting the foregoing, Sparta's security program includes:

Security Awareness and Training. A mandatory security awareness and training program for all Sparta workforce members, including management, covering implementation and compliance with the Information Security Program and promoting a culture of security awareness.

Access Controls. Policies, procedures, and logical controls to limit access to Sparta's information systems to properly authorized persons and to remove access promptly upon changes in job status.

Physical and Environmental Security. Controls providing reasonable assurance that access to physical servers and production environments is limited to authorized individuals, including logging, camera surveillance, environmental monitoring, and backup power systems.

Security Incident Response. A security incident response plan including defined roles and responsibilities, investigation procedures, internal and external notification processes, recordkeeping, and root cause analysis.

Contingency Planning. Policies and procedures for responding to emergencies that could damage Customer Data, including data backups, a formal disaster recovery plan tested at least twice annually, and a business continuity framework.

Endpoint and Device Security. All laptop and desktop computing devices used by Sparta personnel when accessing Customer Data will be equipped with hard disk drive encryption, current anti-virus and anti-malware software, and will be managed using Microsoft Intune and Autopilot as part of Sparta's device management framework, consistent with Sparta's Device Management Playbook.

Microsoft Cloud Security. As a Microsoft Solutions Partner, Sparta delivers services on Microsoft Azure, Microsoft 365, and Dynamics 365. Sparta maintains compliance with Microsoft's shared responsibility model and implements security controls aligned with the Microsoft Cloud Security Benchmark (MCSB) and Zero Trust Architecture principles.

7. Colorado Privacy Act - CPA

This Section documents the safeguard standards imposed to protect Client information subject to the Colorado Privacy Act (6-1-1301). If CPA is identified in the Order, and to the extent Sparta's services constitute processing of personal information governed by CPA, these provisions apply.

Sparta shall adhere to Client's instructions and assist Client in meeting its obligations under the CPA, including by:

- Taking appropriate technical and organizational measures to fulfill Client's obligation to respond to consumer rights requests pursuant to CPA Section 6-1-1306;
- Assisting Client in meeting obligations related to security of processing and breach notification under CPA Section 6-1-716; and
- Providing information to Client necessary to conduct and document data protection assessments required by CPA Section 6-1-1309.

Notwithstanding Client's instructions, Sparta shall:

- Ensure that each person processing personal data is subject to a duty of confidentiality; and
- Engage any subcontractor only after providing Client an opportunity to object, pursuant to a written contract requiring the subcontractor to meet the same obligations as Sparta.

Sparta shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and maintain a clear allocation of responsibilities between Sparta and Client for implementing such measures.

Other State Privacy Laws. To the extent Sparta processes personal data subject to another U.S. state comprehensive privacy or consumer health data law identified in the applicable Order, including without limitation the Oregon Consumer Privacy Act (ORS 646A.570 et seq.) and the Washington My Health My Data Act (chapter 19.373 RCW), Sparta shall, to the extent such law imposes processor or comparable obligations: (a) process such personal data only pursuant to Client’s documented instructions and the Agreement; (b) ensure each person processing such data is subject to a duty of confidentiality; (c) reasonably assist Client in responding to consumer rights requests, meeting security and breach notification obligations, and conducting required data protection assessments; and (d) engage any subcontractor to process such data only pursuant to a written contract imposing obligations no less protective than this DPA, after providing Client an opportunity to object.

8. General Information Security Practices

Regardless of the regulatory frameworks identified in the applicable Order, Sparta maintains the following baseline data protection practices across all client engagements:

a. Microsoft Ecosystem Security

Sparta's managed intelligence delivery is built on Microsoft's trusted cloud infrastructure. Sparta operates under the Microsoft Shared Responsibility Model and maintains:

- Microsoft 365 E-series security controls, including Microsoft Defender, Purview, and Sentinel (as applicable);
- Azure Active Directory / Entra ID with Conditional Access, Multi-Factor Authentication, and Privileged Identity Management;
- Microsoft Intune-based device management with Autopilot enrollment for all managed endpoints;
- Copilot and AI workload controls aligned to Microsoft's Responsible AI Standard and Sparta's AI Acceptable Use Policy; and
- Data residency configurations consistent with Client's geographic and regulatory requirements.

b. Data Classification and Minimization

- Sparta classifies data processed on Client's behalf according to sensitivity and applies controls proportionate to classification.
- Sparta collects and retains only the minimum data necessary to deliver the contracted Services.
- Data retention schedules are defined in the applicable MSA or Service Attachments and honored by Sparta's automated and manual disposal processes.

c. Subcontractor and Partner Controls

- Sparta's services may involve Microsoft subprocessors (e.g., Azure, Microsoft 365) subject to Microsoft's Data Processing Addendum and relevant Standard Contractual Clauses.
- Any non-Microsoft subcontractor engaged in processing Client data will be bound by data protection obligations at least as protective as those in this DPA.
- Sparta will notify Client of any material change to its subcontractor list that affects Client data processing.

d. Audit and Compliance

Audit Rights.

No more than once annually, Client may request information reasonably necessary to verify Provider’s compliance with this DPA.

Provider may satisfy such requests through certifications, audit reports, security summaries, questionnaires, or similar documentation.

Any onsite audit must:

(a) be requested at least thirty (30) days in advance;
(b) occur during normal business hours;
(c) avoid disruption of Provider operations;
(d) be performed by an independent auditor not engaged in competitive activities with Provider; and
(e) be conducted at Client’s sole cost and expense.

9. Term and Termination

a. Term

This Agreement is effective as of the effective date of the applicable Order incorporating it and shall terminate upon the termination of the MSA or upon Client's termination for cause, whichever is sooner.

b. Termination for Cause

Client may terminate this Agreement if Sparta has violated a material term of the Agreement and Sparta has not cured the breach or ended the violation within ten (10) business days of written notice.

c. Effect of Termination

Upon termination of this Agreement for any reason, Sparta shall, with respect to Personal Data received from Client or created or maintained on behalf of Client:

- Retain only that Personal Data which is necessary for Sparta to continue its proper management and administration or to carry out its legal responsibilities;
- Return to Client, or, if agreed to by Client in writing, securely destroy the remaining Personal Data that Sparta still maintains in any form;
- Continue to use appropriate safeguards with respect to retained Personal Data to prevent unauthorized use or disclosure for as long as Sparta retains the Personal Data;
- Not use or disclose retained Personal Data other than for the purposes for which it was retained and subject to the same conditions set forth in this Agreement; and
- Return or destroy retained Personal Data when it is no longer needed for Sparta's proper management and administration or legal responsibilities.

d. Survival

The obligations of Sparta under this Section shall survive the termination of this Agreement.

10. Insurance

In addition to any other insurance required under the Agreement, Client will maintain insurance coverage for privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to data breaches, and legal claims for security breach, privacy violations, and notification costs) in the amount specified in the applicable Order; if no amount is specified, of at least $2,000,000 USD per occurrence.

Sparta maintains professional liability and cyber liability insurance appropriate to the scope and risk profile of its managed intelligence services. Evidence of coverage is available upon written request.

11. Governing Law; Jurisdiction; Hierarchy

Hierarchy.

This DPA is incorporated into and forms part of the MSA.

Except to the extent applicable law requires otherwise, the MSA shall govern in the event of any conflict between this DPA and any other Agreement Document.

Nothing in this DPA shall be interpreted to:

(a) increase Provider's liability;
(b) create liability not otherwise existing under the MSA;
(c) alter the limitation of liability provisions of the MSA;
(d) modify the parties' indemnification obligations under the MSA; or
(e) create any regulatory guarantee or compliance warranty.

All obligations arising under this DPA remain subject to the limitation of liability, disclaimer of warranties, indemnification provisions, and dispute resolution procedures contained in the MSA.