Data Processing Agreement

Effective May 22, 2026. This Data Processing Agreement supersedes and replaces all prior versions.

This Data Processing Agreement (this "**DPA**") is between Methodology IT ("**Provider**") and the Client identified on the applicable Order. It supplements the Master Services Agreement ("MSA"), Service Attachments, and Schedule of Services between Provider and Client (collectively, the "**Agreement**") and governs Provider's processing of Client's regulated data in connection with the Services.

This DPA applies when, and to the extent, Client provides Provider with data subject to one or more privacy or data-protection regimes set forth below. Sections of this DPA become operative only for the regimes applicable to Client's data. Where a particular regime does not apply, the corresponding section is dormant. Capitalized terms not defined in this DPA have the meanings given in the MSA.

If there is a conflict between this DPA and the MSA, this DPA controls with respect to the processing of regulated data. The Order controls over both where there is direct conflict.

---

1. General provisions

1.1 Scope

Provider processes Client Data ("Client Data" as defined in the MSA) solely to deliver the Services. Client Data may include personal information, protected health information, cardholder data, financial information, controlled unclassified information, federal contract information, and similar categories of regulated data depending on Client's business and the framework(s) in scope on the Order.

1.2 Roles

Unless otherwise specified for a specific framework below:

- Client is the **data controller**, **business**, **covered entity**, **financial institution**, or other primary regulated party for its data.
- Provider acts as Client's **data processor**, **service provider**, **business associate**, **service provider under GLBA**, or other secondary party, processing Client Data only on Client's documented instructions and only as needed to deliver the Services.

1.3 Client instructions

The Agreement (this DPA, the MSA, the Schedule of Services, the Order, and applicable Service Attachments) constitutes Client's complete and final documented instructions to Provider for processing Client Data. Any additional or different instructions must be agreed in writing.

1.4 Sub-processors

Provider engages the Third-Party Services Providers identified in the Schedule of Third-Party Services as sub-processors for the corresponding components of the Services. Provider may update the Schedule of Third-Party Services from time to time. Client's acceptance of the Order constitutes general authorization for Provider's use of those sub-processors. Provider will publish updates to the Schedule and, for material additions or substitutions of sub-processors with access to Client's regulated data, Provider will provide reasonable advance notice and Client may object in writing within thirty (30) days, in which case the parties will work in good faith to find a mutually acceptable solution.

Provider's sub-processors are bound by contracts requiring data-protection obligations substantially similar to those in this DPA. Provider remains responsible for sub-processor performance with respect to Client Data.

1.5 Personnel

Provider personnel with access to Client Data are bound by appropriate confidentiality obligations. Provider provides training to personnel handling regulated data.

1.6 Security

Provider maintains administrative, technical, and physical safeguards designed to protect Client Data against unauthorized access, use, disclosure, alteration, or destruction. Provider's security program is described in Provider's Security Practices document published with this DPA and referenced in § 5 below for NY SHIELD purposes. Provider may update its security practices from time to time provided that updates do not materially decrease the level of protection.

1.7 Breach notification

Provider will notify Client without undue delay and in any event within seventy-two (72) hours of confirming a breach of security materially affecting Client Data under Provider's control. Notification will include the nature and scope of the incident, categories and approximate number of affected data subjects and records, likely consequences, and remedial measures taken or proposed. Provider will provide reasonable cooperation to Client in connection with Client's own notification obligations under applicable law.

1.8 Audit and information rights

On reasonable request and no more than once per year (unless required more frequently by law or in response to a confirmed incident), Provider will make available to Client the information reasonably necessary to demonstrate compliance with this DPA. Where Client requires an on-site audit, the audit will be conducted at reasonable times, on reasonable notice, and at Client's expense, subject to confidentiality and security restrictions. Provider may satisfy audit requests with then-current SOC 2, HIPAA, or equivalent third-party reports where available.

1.9 Return or deletion of Client Data

On termination of the Services, Provider will, at Client's choice, return Client Data to Client in a commercially reasonable format or delete Client Data, certifying deletion to Client, except where retention is required by law. Provider's general data-retention obligation under § 3.7 of the MSA also applies.

1.10 Notification of legal requests

If Provider receives a legally binding request for disclosure of Client Data from a government authority or other third party, Provider will, unless legally prohibited, promptly notify Client and provide reasonable opportunity for Client to seek a protective order or other remedy.

---

2. HIPAA — Business Associate Agreement

This § 2 applies when Provider receives, creates, maintains, or transmits Protected Health Information ("**PHI**") on behalf of Client and serves as Client's Business Associate Agreement under HIPAA. Where applicable, Provider is a **Business Associate** and Client is a **Covered Entity** or another Business Associate engaging Provider as a Subcontractor.

2.1 Definitions

Capitalized terms used in this § 2 that are not otherwise defined have the meanings given in the HIPAA Rules (45 CFR Parts 160 and 164), including Breach, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Privacy Rule, Protected Health Information, Required by Law, Secretary, Security Incident, Security Rule, Subcontractor, Unsecured Protected Health Information, and Use.

2.2 Permitted uses and disclosures

Business Associate may use or disclose PHI:

(a) to perform the Services as set forth in the Agreement; (b) for the proper management and administration of Business Associate, or to carry out Business Associate's legal responsibilities,

provided that any such disclosure is required by law or made under reasonable confidentiality assurances; (c) to provide data aggregation services relating to Covered Entity's health care operations as permitted by 45 CFR 164.504(e)(2)(i)(B); (d) to report violations of law to appropriate federal and state authorities consistent with 45 CFR 164.502(j)(1); and (e) to de-identify PHI in accordance with 45 CFR 164.514(a)–(c). De-identified information is not subject to this DPA.

Business Associate will not use or disclose PHI in any way that would violate the Privacy Rule if done by Covered Entity, and will limit its uses and disclosures to the minimum necessary.

2.3 Safeguards

Business Associate will use appropriate administrative, technical, and physical safeguards, and will comply with Subpart C of 45 CFR Part 164 (the Security Rule), to prevent use or disclosure of PHI other than as permitted by this DPA. Business Associate will implement reasonable and appropriate policies and procedures to comply with the Security Rule's requirements for electronic PHI.

2.4 Subcontractors

Business Associate will require its Subcontractors (sub-processors as defined in § 1.4) who create, receive, maintain, or transmit PHI on behalf of Business Associate to agree in writing to substantially the same restrictions and obligations regarding PHI as apply to Business Associate under this § 2.

2.5 Reporting

Business Associate will report to Covered Entity:

(a) any use or disclosure of PHI not permitted by this DPA, of which Business Associate becomes aware, without unreasonable delay and in any event within five (5) business days of discovery; (b) any Security Incident, of which Business Associate becomes aware, in accordance with the timing in (a). Routine unsuccessful attempts at access (port scans, blocked login attempts, pings, etc.) are reported only on Covered Entity's request; and (c) any Breach of Unsecured PHI without unreasonable delay and in any event within five (5) business days of discovery, as required by 45 CFR 164.410. The report will include the information required by 45 CFR 164.410(c).

2.6 Individual rights

Business Associate will:

(a) make PHI in a Designated Record Set available to Covered Entity, or as directed by Covered Entity to an Individual, in the time and manner reasonably necessary for Covered Entity to satisfy its obligations under 45 CFR 164.524; (b) make amendments to PHI in a Designated Record Set as directed by Covered Entity in accordance with 45 CFR 164.526; (c) make available information required to provide an accounting of disclosures in accordance with 45 CFR 164.528; and (d) to the extent Business Associate is to carry out one or more of Covered Entity's obligations under Subpart

E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to Covered Entity in performing such obligation(s).

2.7 HHS access

Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA Rules.

2.8 Termination and return of PHI

On termination of the Services, Business Associate will, at Covered Entity's choice, return or destroy all PHI received from, or created or received on behalf of, Covered Entity that Business Associate maintains in any form. If return or destruction is infeasible, Business Associate will extend the protections of this DPA to such PHI and limit further uses and disclosures to those purposes that make return or destruction infeasible.

2.9 Notice of privacy practices

Covered Entity will notify Business Associate of: (a) any limitation(s) in Covered Entity's Notice of Privacy Practices under 45 CFR 164.520 that may affect Business Associate's use or disclosure of PHI; (b) any changes in or revocation of an Individual's permission to use or disclose PHI; and (c) any restriction on the use or disclosure of PHI that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent any of the foregoing affect Business Associate's use or disclosure of PHI.

2.10 Permissible requests

Covered Entity will not request Business Associate to use or disclose PHI in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity, except as permitted in § 2.2(b) and (c).

---

3. State consumer privacy laws (CCPA / CPRA and comprehensive state privacy regimes)

This § 3 applies when Client provides Provider with Personal Information regulated by a U.S. state consumer privacy law — including the California Consumer Privacy Act as amended by the California Privacy Rights Act ("**CCPA/CPRA**"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Texas Data Privacy and Security Act, the Oregon Consumer Privacy Act, the Montana Consumer Data Privacy Act, the Tennessee Information Protection Act, the Delaware Personal Data Privacy Act, the New Jersey Data

Privacy Act, the Iowa Consumer Data Protection Act, and any other comparable state law in effect (collectively, "**State Privacy Laws**").

3.1 Definitions

For purposes of this § 3, capitalized terms not otherwise defined have the meanings given in the applicable State Privacy Law. "**Personal Information**" means data regulated under the applicable State Privacy Law that Provider processes on Client's behalf in connection with the Services.

3.2 Roles

Client acts as "Business" (under the CCPA/CPRA) or "Controller" (under other State Privacy Laws). Provider acts as "Service Provider" (under the CCPA/CPRA) or "Processor" (under other State Privacy Laws). Provider receives Personal Information for the limited and specified business purpose of providing the Services.

3.3 No sale or sharing

Provider will not sell or share Personal Information as those terms are defined under the CCPA/CPRA, and will not otherwise transfer Personal Information for monetary or other valuable consideration to any third party except as authorized by Client to deliver the Services.

3.4 Limitations on use and disclosure

Provider will:

(a) process Personal Information only for the business purposes identified in the Agreement and as needed to deliver the Services; (b) not retain, use, or disclose Personal Information for any purpose other than performing the Services or as otherwise permitted by law; (c) not retain, use, or disclose Personal Information outside the direct business relationship between Provider and Client, except as permitted by law; (d) not combine Personal Information that Provider receives from or on behalf of Client with personal information received from or on behalf of another entity, except as permitted by law and to perform the Services; and (e) comply with the obligations applicable to a "Service Provider" or "Processor" under the applicable State Privacy Law.

3.5 Sensitive personal information

Where Personal Information includes "Sensitive Personal Information" or analogous categories of sensitive data under State Privacy Laws, Provider will not use that data for advertising, profiling, or any purpose other than the specific business purpose of providing the Services.

3.6 Data subject rights

Provider will reasonably assist Client in responding to verifiable consumer rights requests (access, deletion, correction, portability, opt-out of sale or sharing, opt-out of profiling, limitation of use of

sensitive data, and other rights afforded under the applicable State Privacy Law). If Provider receives a consumer rights request directly, Provider will not respond substantively and will forward the request to Client without undue delay.

3.7 Data protection assessments

Provider will reasonably assist Client in preparing data protection assessments or risk assessments required under applicable State Privacy Laws by providing relevant information about Provider's processing activities on Client's behalf.

3.8 Subcontractor flow-down

Provider will impose obligations on its sub-processors under § 1.4 substantially equivalent to those in this § 3 to the extent they process Personal Information.

3.9 Certification

Provider certifies that it understands and will comply with the restrictions and obligations set out in this § 3, including the certifications required by Section 1798.140(ag)(1) of the CCPA/CPRA.

---

4. GLBA — financial services data

This § 4 applies when Provider processes Nonpublic Personal Information ("**NPI**") regulated by the Gramm-Leach-Bliley Act and the FTC Safeguards Rule (16 CFR Part 314).

4.1 Receipt of information

Provider is authorized to receive, hold, and use NPI to perform the Services as directed by Client.

4.2 Obligations

Provider will:

(a) implement and maintain a written, comprehensive information security program containing the administrative, technical, and physical safeguards required by 16 CFR Part 314; (b) ensure the security and confidentiality of NPI; (c) protect against anticipated threats or hazards to the security and integrity of NPI; (d) protect against unauthorized access to or use of NPI that could result in substantial harm or inconvenience to consumers; (e) ensure the secure disposal of NPI as required by applicable law; and (f) notify Client of any unauthorized access to or breach of NPI in accordance with the breach-notification timing in § 1.7.

4.3 Permitted uses

Provider will use or disclose NPI only as necessary to perform the Services or as required by law.

4.4 Permissible requests

Client will not request Provider to use or disclose NPI in a manner that would not be permissible under Title V of the Gramm-Leach-Bliley Act and the regulations issued thereunder if done by Client.

---

5. NY SHIELD Act and state cybersecurity requirements

This § 5 applies where Client is subject to the New York Stop Hacks and Improve Electronic Data Security Act ("**SHIELD Act**") or to analogous state-level cybersecurity statutes (including Massachusetts 201 CMR 17.00, Texas Business and Commerce Code Chapter 521, the Florida Information Protection Act, and similar). Provider maintains a comprehensive written information security program with administrative, technical, and physical safeguards appropriate to the size, scope, and type of Provider's business and the sensitivity of the data Provider handles. Provider's program is designed to:

- Protect the confidentiality, integrity, and availability of Client Data in Provider's possession or control;
- Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of Client Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Client Data;
- Protect against accidental loss, destruction, or damage to Client Data; and
- Satisfy applicable cybersecurity safeguards required by state, federal, or industry-specific regulations.

The program includes the security control categories described in Provider's published Security Practices document — security awareness training, access controls, physical and environmental security, security incident procedures, contingency planning, audit controls, data integrity, storage and transmission security, secure disposal, assigned security responsibility, regular testing, monitoring, change management, program adjustments, and endpoint security.

For Clients subject to the New York Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500), Provider's controls are designed to support Client's compliance with that regulation in accordance with the Service Attachment for Managed Compliance Services where applicable.

---

6. GDPR and UK GDPR (where applicable)

This § 6 applies where Provider processes Personal Data (as defined in the EU General Data Protection Regulation or UK GDPR) that pertains to data subjects in the European Economic Area, the United Kingdom, or Switzerland, or where Client is otherwise subject to the GDPR or UK GDPR in connection with the Services.

6.1 Roles

Client is the "Controller" (or, where applicable, a "Processor" engaging Provider as a Sub-processor). Provider is the "Processor" (or "Sub-processor"). Provider processes Personal Data only on documented instructions from Client.

6.2 Technical and organizational measures

Provider implements technical and organizational measures appropriate to the risk in accordance with GDPR Article 32, including pseudonymization and encryption where appropriate, measures to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems, measures to restore availability and access to Personal Data in a timely manner after an incident, and a process for regularly testing and evaluating the effectiveness of those measures.

6.3 Sub-processors

Provider's use of sub-processors is governed by § 1.4. Provider's sub-processors are bound to data protection obligations substantially similar to those imposed on Provider under this § 6, providing sufficient guarantees that processing will meet the requirements of the GDPR.

6.4 Confidentiality of personnel

Provider will ensure that persons authorized to process Personal Data are subject to appropriate confidentiality obligations.

6.5 Cooperation with Client

Provider will reasonably assist Client, taking into account the nature of the processing and the information available to Provider, in:

(a) responding to data subject rights requests (GDPR Articles 15–22); (b) ensuring compliance with the obligations on personal data breaches (Articles 33 and 34), data protection impact assessments (Article 35), and prior consultation (Article 36); (c) demonstrating compliance with the GDPR.

6.6 Breach notification

Personal Data Breaches are notified to Client per § 1.7.

6.7 Cross-border transfers

Where Personal Data is transferred from the EEA, the UK, or Switzerland to a country not recognized by the European Commission, UK government, or Swiss Federal Council as providing an adequate level of data protection, the parties will rely on the most current Standard Contractual Clauses ("**SCCs**") or UK International Data Transfer Addendum, incorporated by reference into this DPA. Where the parties have completed the optional SCC Appendix (Annex 1 below) and the UK Addendum (where applicable), those instruments govern the transfer.

6.8 Records and audits

Provider will maintain records of processing activities required by GDPR Article 30(2), to the extent applicable, and will make them available to Client on reasonable request, subject to confidentiality protections and the audit framework in § 1.8.

6.9 Return or deletion

On termination, Provider will return or delete Personal Data as directed by Client, in accordance with § 1.9, unless retention is required by EU or member state law.

6.10 Compliance assistance fees

Provider's GDPR compliance assistance under this DPA is included in the Services to a reasonable extent. Substantial assistance (extended data subject rights responses, full data audits, complex transfers analysis, regulator interactions) is billable at Provider's then-current hourly rates as Project Services.

---

7. General

7.1 Limitation of liability

Provider's liability under this DPA is subject to the Limitation of Liability set forth in the MSA.

7.2 Conflict resolution

If a conflict arises between this DPA and a regulator or supervisory authority's interpretation of an applicable framework, the parties will work in good faith to bring this DPA into alignment. Provider may update this DPA on reasonable notice to reflect changes in applicable law.

7.3 Survival

Provisions of this DPA that by their nature should survive termination — including breach notification, return of data, audit rights, and HIPAA-required obligations — survive termination.

7.4 Order of precedence

Within the Agreement, the order of precedence is: Order; this DPA (for regulated-data processing); any applicable Service Attachment; the Schedule of Services; the MSA; the Schedule of Third-Party Services.

7.5 No third-party beneficiaries

Except as required by applicable law (for example, data-subject rights under GDPR Article 28, beneficiary rights under SCCs), this DPA is for the benefit of the parties and does not create third-party beneficiary rights.

7.6 Updates

Provider may update this DPA from time to time, with at least sixty (60) days' written notice for material changes that increase Client's obligations or reduce Client's protections. Non-material updates (clarifications, citations to current law, references to updated sub-processor lists) may be made without notice.

Annex 1 — Description of processing (for GDPR / SCCs)

This Annex is completed only where the parties are relying on the SCCs for a cross-border transfer of Personal Data. Where not completed, this Annex is dormant.

Categories of data subjects: *[populated per Client Order — typically Client's employees, customers, and other individuals interacting with Client's systems managed by Provider]*

Categories of personal data: *[populated per Client Order — typically identification, contact, employment, technical, and behavioral data necessary for the Services]*

Special categories of data: *[populated per Client Order — none unless explicitly identified]*

Frequency of transfer: Continuous, for the duration of the Services.

Nature of processing: Hosting, monitoring, security operations, identity and access management, backup and recovery, and other activities described in the Schedule of Services and applicable Service Attachments.

Purpose of transfer and processing: Delivery of the Services to Client.

Retention period: For the duration of the Services and subject to return or deletion on termination per § 1.9.

Sub-processors: As set forth in the Schedule of Third-Party Services.

Competent supervisory authority: As determined under GDPR Article 56 and the parties' arrangement.

Annex 2 — Technical and organizational measures (for GDPR / SCCs and NY SHIELD reference)

Provider's technical and organizational measures are described in Provider's Security Practices document published with this DPA. Measures include, at a minimum:

- Access control to managed systems, with multi-factor authentication for privileged access
- Encryption in transit (TLS 1.2+) and encryption at rest where the underlying platform supports it
- Logging and monitoring of administrative access to managed systems
- Vulnerability and patch management programs aligned to Provider's standard policies
- Security awareness training for personnel handling regulated data
- Background checks for personnel with access to regulated data
- Incident response procedures with defined escalation
- Physical security at Provider locations, including controlled access
- Sub-processor risk management including contracts requiring equivalent obligations
- Business continuity and disaster recovery procedures
- Annual review and update of security program

Acceptance.

This DPA is incorporated into the Agreement by reference upon Client's acceptance of the Order. Where Client provides Provider with regulated data covered by a section of this DPA, that section becomes operative without further action by the parties. Provider may publish updated versions of this DPA on Provider's website; the version in effect at the time of any particular processing activity governs that activity, subject to the change-notice provisions in § 7.6.