

## Exhibit D – Data Protection Addendum

### DATA PROTECTION ADDENDUM

This Data Protection Addendum (“DPA”) supplements and is incorporated into the Agreement. This DPA governs Contractor’s Processing of Personal Information on behalf of OCERS in connection with the Agreement.

In the event of any conflict between this DPA and the Agreement with respect to the Processing of Personal Information, this DPA shall control. With respect to all other matters, the Agreement shall control. Nothing in this DPA reduces, limits, or supersedes the protections that the Agreement affords to OCERS Data generally; this DPA provides additional, privacy-specific obligations applicable to Personal Information.

#### 1. DEFINITIONS

Capitalized terms used and not otherwise defined in this DPA have the meanings given in the Agreement. The following additional terms apply:

“**ADMT**” or “Automated Decisionmaking Technology” has the meaning set forth in 11 CCR § 7001.

“**CCPA**” means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 and as amended from time to time, together with its implementing regulations at Title 11, Division 6, of the California Code of Regulations (“CCPA Regulations”).

“**Consumer**” has the meaning set forth in California Civil Code § 1798.140(i).

“**Cross-Context Behavioral Advertising**” has the meaning set forth in California Civil Code § 1798.140(k).

“**CMIA**” means the California Confidentiality of Medical Information Act (Civil Code § 56 et seq.).

“**CPPA**” means the California Privacy Protection Agency.

“**Cybersecurity Audit**” means the cybersecurity audit required under 11 CCR §§ 7120–7124 and any successor regulation.

“**Data Subject**” means a natural person whose Personal Information is Processed under the Agreement, including OCERS members, beneficiaries, applicants, retirees, employees, Board members, and other individuals whose Personal Information OCERS provides or makes accessible to Contractor.

“**Permitted Purpose**” means each business purpose for which OCERS has authorized Contractor to Process Personal Information, as identified in Schedule 1 (Description of Processing) and the Agreement.

“**Personal Information**” or “PI” has the meaning set forth in California Civil Code § 1798.140(v) and includes Sensitive Personal Information.

“**Process**” or “Processing” has the meaning set forth in California Civil Code § 1798.140(y) and includes any operation or set of operations performed on Personal Information, including collection, use, storage, disclosure, transfer, alteration, retention, and deletion.

“**Risk Assessment**” means the risk assessment required under 11 CCR §§ 7150–7157 and any successor regulation.

“**Sell**” and “**Share**” have the meanings set forth in California Civil Code § 1798.140(ad) and (ah), respectively.

**“Sensitive Personal Information”** or “SPI” has the meaning set forth in California Civil Code § 1798.140(ae).

**“Service Provider”** and **“Contractor”** (as a CCPA term, distinct from the contracting party) have the meanings set forth in California Civil Code § 1798.140(ag) and (j), respectively.

**“Significant Decision”** has the meaning set forth in 11 CCR § 7001.

**“Subcontractor”** means any third party engaged by Contractor (including any affiliate of Contractor) to Process Personal Information in connection with the Agreement.

## **2. ROLES OF THE PARTIES**

**2.1 OCERS as a Public Retirement System.** OCERS is a public retirement system organized and operating under the County Employees Retirement Law of 1937 (Government Code § 31450 et seq.). OCERS does not act as a “Business” as defined in California Civil Code § 1798.140(d), because OCERS is not organized or operated for the profit or financial benefit of shareholders or other owners. Notwithstanding the foregoing, Contractor agrees to comply with the obligations applicable to a “Service Provider” or “Contractor” under the CCPA and 11 CCR § 7050 et seq. as if OCERS were a Business, in addition to all other obligations applicable to OCERS as a public agency. OCERS makes Personal Information available to Contractor solely for the Permitted Purposes.

**2.2 Contractor as Service Provider or Contractor.** Contractor Processes Personal Information on behalf of OCERS as a “Service Provider” or “Contractor” within the meaning of California Civil Code §§ 1798.140(ag), 1798.140(j), and 11 CCR § 7050 et seq. Contractor shall not act as a “Third Party” as defined in California Civil Code § 1798.140(ai) with respect to Personal Information Processed under the Agreement.

**2.3 No Joint Controllership; No Sale.** The disclosure of Personal Information by OCERS to Contractor does not constitute a Sale or a Share of Personal Information and is made solely for the limited and specified Permitted Purposes set forth in this DPA and the Agreement. Contractor shall not characterize, treat, or hold itself out as a joint Business or controller of Personal Information Processed under the Agreement.

## **3. PERMITTED PURPOSES**

**3.1 Business Purposes.** Contractor shall Process Personal Information solely for the Permitted Purposes specified in Schedule 1 and the Agreement, and for no other purpose. The Permitted Purposes constitute “business purposes” as that term is used in California Civil Code § 1798.140(e) and 11 CCR § 7050.

**3.2 Direct Business Relationship.** Contractor shall not Process Personal Information outside of the direct business relationship between Contractor and OCERS.

**3.3 OCERS Instructions.** Contractor shall Process Personal Information only on documented instructions from OCERS, including the Agreement, this DPA, Schedule 1, written change orders, and other written directions from OCERS’ designated representative. If Contractor reasonably believes that an instruction violates applicable law, Contractor shall promptly notify OCERS in writing and, except where applicable law prohibits, suspend the Processing pending resolution.

## **4. PROHIBITED USES OF PERSONAL INFORMATION**

Contractor shall not, and shall not permit any Subcontractor or other person under its control to:

- (a) Sell or Share any Personal Information;

- (b) Retain, use, or disclose any Personal Information for any purpose other than the Permitted Purposes specified in Schedule 1 and the Agreement, including for any commercial purpose other than performing the Services for OCERS;
- (c) Retain, use, or disclose any Personal Information outside of the direct business relationship between Contractor and OCERS;
- (d) Combine Personal Information that Contractor receives from or on behalf of OCERS with Personal Information that Contractor receives from or on behalf of any other person or entity, or collects from its own interactions with consumers, except that Contractor may combine such Personal Information solely to the extent necessary to perform a business purpose enumerated in 11 CCR § 7050(b)(1)–(7) and as expressly authorized by OCERS in writing;
- (e) Use any Personal Information, Sensitive Personal Information, derived data, metadata, prompts, inputs, outputs, model embeddings, vectors, telemetry, logs, or feedback artifacts to develop, train, fine-tune, evaluate, or improve any artificial intelligence model or system, whether Contractor’s own or a third party’s, or any product or service unrelated to the Permitted Purposes, in each case without OCERS’ prior express written consent;
- (f) Use Personal Information for Cross-Context Behavioral Advertising, profiling for marketing or commercial purposes, or any analogous secondary use;
- (g) Disclose Personal Information to any third party other than (i) Subcontractors approved under Section 8 (Subcontractors) and bound by obligations consistent with this DPA, (ii) as compelled by valid legal process subject to the notice obligations in Section 9 (Compelled Disclosures), or (iii) as expressly directed in writing by OCERS;
- (h) Retain Personal Information for any period longer than is reasonably necessary to perform the Permitted Purposes, except as required by applicable law or as expressly authorized in writing by OCERS; or
- (i) Use any Personal Information for the personal benefit of any officer, employee, agent, or Subcontractor of Contractor.

## **5. SAME LEVEL OF PRIVACY PROTECTION**

**5.1 Compliance with the CCPA.** Contractor shall comply with all applicable provisions of the CCPA, the CCPA Regulations, and any other applicable California, federal, and local privacy and data protection laws.

**5.2 CERL Confidentiality of Member Records.** Contractor acknowledges that the records of OCERS members are confidential under California Government Code § 31532 and may not be disclosed except (a) as necessary for the administration of CERL, (b) upon order of a court of competent jurisdiction, or (c) upon the written authorization of the affected member. Contractor shall handle all Personal Information of OCERS members and beneficiaries consistent with the requirements of Government Code § 31532, in addition to all other confidentiality and security obligations under this DPA and the Agreement.

**5.3 Medical Information; CMIA; HIPAA.** (a) “Medical Information” has the meaning set forth in California Civil Code § 56.05(j). To the extent the Services involve Processing of Medical Information of any OCERS member, beneficiary, applicant, retiree, employee, or other individual, Contractor shall comply with the California Confidentiality of Medical Information Act (Civil Code § 56 et seq.) (“CMIA”) in addition to all other obligations under this DPA. Without limiting the foregoing, Contractor shall: (i) not use, disclose, or further Process Medical Information except as expressly permitted by CMIA and as necessary to perform the Permitted Purposes; (ii) implement administrative, technical, and physical safeguards appropriate to the sensitivity of Medical Information and consistent with industry standards for the handling of patient medical records; (iii) limit access to Medical Information to personnel and Subcontractors with a

legitimate need to know based on the Permitted Purposes; (iv) maintain logs sufficient to support CMIA accounting of disclosures; (v) cooperate with OCERS in responding to authorization requests, member inquiries, and any breach notification obligations under Civil Code § 56.36; and (vi) acknowledge that Contractor may be subject to the civil penalties and remedies under Civil Code § 56.36 for violations. (b) HIPAA Business Associate Agreement. If Contractor is a “Covered Entity” or “Business Associate” under HIPAA (45 CFR § 160.103) with respect to the Services or any Personal Information Processed under the Agreement, or if any third party providing services to OCERS through Contractor is so situated, the Parties shall execute a Business Associate Agreement in a form mutually agreed by the Parties, which shall govern Contractor’s handling of Protected Health Information as defined in HIPAA. The Parties acknowledge that OCERS itself is not a HIPAA Covered Entity but may receive Medical Information from sources subject to HIPAA, and that the appropriate vehicle for HIPAA compliance depends on Contractor’s status. (c) Other Specialized Privacy Regimes. If and to the extent the Services involve Processing of financial information subject to the Gramm-Leach-Bliley Act, or other specialized privacy regimes, Contractor shall comply with each such regime applicable to the Personal Information at issue.

**5.4 Notification of Inability to Comply.** Contractor shall notify OCERS in writing no later than five (5) business days after Contractor makes a determination that it can no longer meet its obligations under the CCPA, the CCPA Regulations, or this DPA. The notification shall describe the obligation Contractor cannot meet, the reason, the date the inability commenced, and Contractor’s proposed remediation. This obligation implements 11 CCR § 7051(a)(7).

**5.5 Compliance Certification on Request.** On OCERS’ written request, Contractor shall provide OCERS with a written certification, signed by an authorized officer of Contractor, that Contractor has complied with this DPA and the CCPA Regulations during the period specified in OCERS’ request. This certification supports OCERS’ verification of compliance under 11 CCR § 7051(a)(5).

## **6. ASSISTANCE WITH OCERS’ COMPLIANCE OBLIGATIONS**

**6.1 OCERS Member Rights Requests.** Contractor shall provide OCERS with reasonable cooperation and assistance, at no additional charge, to enable OCERS to respond to requests from OCERS members, beneficiaries, employees, and other Data Subjects to access, correct, or obtain information about their Personal Information held by or Processed through the Services. Contractor shall implement OCERS-directed responses (including correction or deletion, where lawful) in production systems within ten (10) business days of OCERS’ request, and shall propagate such responses to all systems, backups, and Subcontractors as required by applicable law. Nothing in this Section creates rights enforceable directly by Data Subjects against Contractor; Contractor’s obligations under this Section run solely to OCERS.

**6.2 Risk Assessments.** If OCERS is required to conduct a Risk Assessment under 11 CCR §§ 7150–7157 (or successor regulation) with respect to Processing performed by Contractor, Contractor shall provide all information reasonably requested by OCERS to enable OCERS to complete the Risk Assessment, including information regarding (a) the categories of Personal Information Processed; (b) the operational elements of the Processing; (c) the safeguards in place; (d) the benefits and risks to consumers; (e) the use of any ADMT; and (f) any sub-processing arrangements.

**6.3 Cybersecurity Audits.** If OCERS is required to conduct or commission a Cybersecurity Audit under 11 CCR §§ 7120–7124 (or successor regulation) covering Processing performed by Contractor, Contractor shall provide reasonable cooperation, including (a) access to relevant policies, procedures, and records; (b) responses to auditor questionnaires; (c) interviews with personnel; and (d) any independent third-party audit reports relevant to the Cybersecurity Audit scope. Contractor shall designate a cybersecurity audit point of contact in Schedule 1.

**6.4 Automated Decisionmaking Technology.** (a) If Contractor uses or makes available any ADMT in connection with the Services, Contractor shall identify each such ADMT in Schedule 1 and shall not deploy any new ADMT for any Significant Decision concerning a Data Subject without OCERS' prior written approval. (b) Contractor shall provide all information and operational support reasonably necessary to enable OCERS to satisfy any pre-use notice, access, opt-out, and appeal obligations under 11 CCR §§ 7200–7227 (or successor regulation), including providing meaningful information about the logic, intended outputs, and outputs of the ADMT. (c) Contractor shall maintain logs sufficient to enable OCERS to identify the ADMT outputs that contributed to any Significant Decision concerning a Data Subject and to provide individualized disclosures upon request.

**6.5 Notices and Cooperation Generally.** Contractor shall provide OCERS with all information reasonably necessary to enable OCERS to demonstrate compliance with the CCPA and to respond to inquiries from the CPPA, the California Attorney General, or any other governmental or regulatory authority. Contractor shall promptly forward to OCERS any communication from a Data Subject, the CPPA, the California Attorney General, or any other governmental authority that relates to Personal Information Processed under the Agreement.

## **7. SECURITY OF PERSONAL INFORMATION**

**7.1 Reasonable Security.** Contractor shall implement and maintain reasonable security procedures and practices appropriate to the nature of the Personal Information, in compliance with California Civil Code § 1798.81.5, the security obligations of the Agreement, and (where applicable) any Security Requirements exhibit attached to the Agreement. This obligation implements 11 CCR § 7051(a)(10).

**7.2 Sensitive Personal Information.** With respect to Sensitive Personal Information, Contractor shall implement enhanced security measures appropriate to the heightened sensitivity of such information, including encryption at rest and in transit, multi-factor authentication for all access, role-based access controls, comprehensive logging, and access on a least-privilege, need-to-know basis.

**7.3 Personnel.** Contractor shall ensure that any personnel authorized to Process Personal Information are bound by written confidentiality obligations and have received training on Contractor's privacy and security obligations under this DPA and applicable law.

**7.4 Security Incidents.** Contractor shall notify OCERS of any Security Incident affecting Personal Information in accordance with the Security Incident notification provisions of the Agreement. In addition, Contractor shall (a) promptly provide OCERS with the categories of Personal Information and Sensitive Personal Information affected and the number of affected Data Subjects, by category, to the extent reasonably ascertainable; (b) cooperate with OCERS' fulfillment of breach notification obligations under California Civil Code §§ 1798.29 and 1798.82, the CMIA, HIPAA, or other applicable law; and (c) at OCERS' direction and at Contractor's expense, draft and send (or reimburse OCERS for the costs of drafting and sending) the breach notifications required by law.

## **8. SUBCONTRACTORS**

**8.1 Approval and Notice.** Contractor shall not engage any Subcontractor to Process Personal Information without OCERS' prior written approval. The Subcontractors approved as of the effective date of this DPA are listed in Schedule 1. Contractor shall provide OCERS with at least thirty (30) days' prior written notice of any proposed change in Subcontractors, during which OCERS may object on reasonable grounds. This obligation implements 11 CCR § 7051(a)(11) and 11 CCR § 7053.

**8.2 Flow-Down.** Contractor shall enter into a written agreement with each Subcontractor that imposes obligations on the Subcontractor that are no less protective of Personal Information than those imposed on Contractor under this DPA, including all of the obligations required by 11 CCR § 7051(a) and 11 CCR § 7053. Contractor shall make a copy of each such Subcontractor agreement available to OCERS on reasonable request, with such redactions as are reasonable to protect commercially sensitive information.

**8.3 Liability.** Contractor shall remain fully liable to OCERS for the acts and omissions of each Subcontractor as if such acts or omissions were those of Contractor.

## **9. COMPELLED DISCLOSURES**

If Contractor receives a subpoena, court order, search warrant, civil investigative demand, regulatory inquiry, or other compulsory legal process seeking disclosure of Personal Information, Contractor shall: (a) unless legally prohibited, provide OCERS with prompt written notice and a copy of the demand sufficient to allow OCERS to seek a protective order or other appropriate relief; (b) reasonably cooperate with OCERS' efforts to limit, quash, or modify the demand; (c) disclose only the minimum Personal Information legally required; and (d) where notice is legally prohibited, use reasonable efforts to challenge the prohibition and to provide notice as soon as legally permissible. Contractor shall not voluntarily disclose Personal Information to any government authority absent OCERS' prior written authorization or a binding legal compulsion.

## **10. OCERS' OVERSIGHT AND REMEDIATION RIGHTS**

**10.1 Right to Take Reasonable Steps.** OCERS has the right to take reasonable and appropriate steps to ensure that Contractor uses Personal Information in a manner consistent with OCERS' obligations under the CCPA. This right implements 11 CCR § 7051(a)(6).

**10.2 Right to Stop and Remediate Unauthorized Use.** Upon notice to Contractor, OCERS has the right to take reasonable and appropriate steps to stop and remediate any unauthorized use of Personal Information by Contractor or any Subcontractor. Such steps may include suspending Contractor's access to Personal Information, requiring Contractor to delete or return Personal Information, requiring Contractor to engage independent assessors, and exercising any other rights of OCERS under this DPA, the Agreement, or applicable law. This right implements 11 CCR § 7051(a)(8).

**10.3 Audit Rights.** In addition to the audit rights set forth in the Agreement, OCERS (or its independent auditors or consultants) shall have the right, upon reasonable prior written notice and during normal business hours, to audit Contractor's compliance with this DPA. Contractor shall cooperate in good faith and provide reasonable access to personnel, records, policies, procedures, and facilities relevant to the audit. Audits shall be conducted no more than once per calendar year except (a) following a Security Incident affecting Personal Information, (b) following OCERS' receipt of credible information indicating non-compliance, or (c) as required by a governmental or regulatory authority. OCERS shall bear its own audit costs unless the audit identifies a material non-compliance, in which case Contractor shall reimburse OCERS' reasonable audit costs and promptly remediate the non-compliance.

**10.4 Records of Processing.** Contractor shall maintain accurate and current records of its Processing of Personal Information sufficient to demonstrate compliance with this DPA, including records reflecting the categories of Personal Information Processed, the Permitted Purposes, the Subcontractors engaged, the security measures implemented, and any material changes thereto. Contractor shall provide such records to OCERS on reasonable request.

## **11. DATA RESIDENCY**

Contractor shall store and Process Personal Information only within the United States. Contractor shall not transfer or permit the transfer of Personal Information outside the United States, or allow access to Personal Information from outside the United States, without OCERS' prior written consent. The hosting locations approved as of the effective date of this DPA are listed in Schedule 1.

## **12. RETURN AND DELETION OF PERSONAL INFORMATION**

**12.1 Return and Deletion Generally.** On expiration or termination of the Agreement, or earlier at OCERS' written request, Contractor shall return to OCERS, in a format requested by OCERS, all Personal Information in Contractor's possession or control, and shall thereafter securely delete all copies of Personal Information from Contractor's systems (including those of Subcontractors) in accordance with NIST SP 800-88 or comparable standard. Contractor shall certify deletion in writing to OCERS within thirty (30) days of completion. The return-and-deletion obligations of the Agreement, including any transition assistance period, shall apply to Personal Information.

**12.2 Limited Retention Exception.** If Contractor is required by applicable law to retain any Personal Information beyond the termination of the Agreement, Contractor shall (a) provide OCERS with written notice identifying the retention obligation and the categories of Personal Information retained; (b) maintain such Personal Information in confidence subject to the protections of this DPA; (c) use such Personal Information solely for the purpose giving rise to the retention obligation; (d) implement reasonable measures to isolate and secure such Personal Information; and (e) delete such Personal Information promptly upon expiration of the legal retention obligation.

**12.3 Backups.** Backup copies of Personal Information that cannot be selectively deleted shall be (a) isolated and protected from any further Processing, (b) used solely for disaster recovery purposes, and (c) deleted in the ordinary course in accordance with Contractor's backup retention schedule disclosed to OCERS, but in no event longer than ninety (90) days after termination of the Agreement, unless a longer period is required by applicable law.

## **13. INDEMNIFICATION AND LIABILITY**

Contractor's indemnification obligations and liability for breach of this DPA are governed by the indemnification and limitation-of-liability provisions of the Agreement. For the avoidance of doubt, breach of this DPA constitutes a breach of Contractor's data protection obligations and a breach of confidentiality under the Agreement. Liability arising from breach of this DPA is among the matters that, under the Agreement, are not subject to the cap on aggregate liability.

## **14. GENERAL PROVISIONS**

**14.1 Term and Survival.** This DPA takes effect on the effective date of the Agreement (or such later date as the Parties execute this DPA, if separately executed) and continues for the duration of the Agreement and for so long as Contractor Processes Personal Information. The provisions of this DPA that by their nature should survive termination, including Sections 4 (Prohibited Uses), 5.4 (Notification), 7.4 (Security Incidents), 9 (Compelled Disclosures), 10 (Oversight), 12 (Return and Deletion), and 13 (Indemnification), shall survive.

**14.2 Order of Precedence.** This DPA controls over the Agreement with respect to the Processing of Personal Information. With respect to all other matters, the Agreement controls. If a more recent applicable California or federal privacy law or regulation imposes obligations more protective of Personal

Information than those in this DPA, the more protective obligations shall apply, and the Parties shall negotiate in good faith any DPA amendments necessary to reflect those obligations.

**14.3 Regulatory Updates.** The Parties acknowledge that the CCPA Regulations are evolving, including with respect to ADMT (11 CCR §§ 7200–7227), Risk Assessments (11 CCR §§ 7150–7157), and Cybersecurity Audits (11 CCR §§ 7120–7124). The Parties shall cooperate in good faith to amend this DPA as reasonably necessary to address phased compliance dates and final regulatory requirements.

**14.4 California Public Records Act.** Contractor acknowledges that OCERS is subject to the California Public Records Act (Government Code § 7920.000 et seq.). Nothing in this DPA prevents OCERS from disclosing Personal Information to the extent required by the California Public Records Act or other applicable law, subject to the redactions and exemptions provided by law.

**14.5 No Waiver of Public-Agency Rights or Immunities.** Nothing in this DPA waives, modifies, or limits any immunity, defense, privilege, or procedural protection available to OCERS as a public agency under the California Government Claims Act (Government Code § 810 et seq.), CERL, the California Public Records Act, or other applicable law.

**14.6 Amendment.** This DPA may be amended only by a written instrument signed by authorized representatives of both Parties.

**14.7 Counterparts; Electronic Signatures.** This DPA may be signed in counterparts and delivered electronically in accordance with the California Uniform Electronic Transactions Act (Civil Code § 1633.1 et seq.). An electronic signature has the same legal force and effect as an original handwritten signature.

**14.8 No Third-Party Beneficiaries.** This DPA is for the benefit of the Parties only and creates no rights enforceable by any third party, except that Data Subjects may have rights under the CCPA and other applicable law that are independent of this DPA.

**14.9 Severability.** If any provision of this DPA is held invalid or unenforceable, the remaining provisions shall remain in full force and effect, and the invalid or unenforceable provision shall be replaced with a valid and enforceable provision that most closely reflects the original intent.



## **SCHEDULE 1**

### **Description of Processing**

*[To be completed for each engagement.]*

#### **A. Subject Matter and Duration of Processing.**

Subject matter: \_\_\_\_\_

Duration: For the term of the Agreement and any transition assistance period, plus any retention period required by applicable law as identified below.

#### **B. Permitted Purposes (Business Purposes).**

Contractor is authorized to Process Personal Information solely for the following Permitted Purposes, each of which is a “business purpose” under California Civil Code § 1798.140(e) and 11 CCR § 7050:

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_

#### **C. Categories of Data Subjects.**

*[Check all that apply.]*

- ☐ OCERS members (active, deferred, retired)
- ☐ Beneficiaries and dependents
- ☐ Applicants for membership or benefits
- ☐ OCERS employees
- ☐ OCERS Board members and trustees
- ☐ OCERS contractors and consultants
- ☐ Other (specify): \_\_\_\_\_

#### **D. Categories of Personal Information.**

*[Check all that apply.]*

- ☐ Identifiers (name, address, SSN, member ID, email, phone)
- ☐ California Customer Records categories (Civil Code § 1798.80(e))
- ☐ Protected classifications under California or federal law
- ☐ Commercial information
- ☐ Internet or other electronic network activity information
- ☐ Geolocation data
- ☐ Audio, electronic, visual, or similar information
- ☐ Professional or employment-related information

- ☐ Education information (FERPA-covered)
- ☐ Inferences drawn from other Personal Information
- ☐ Other (specify): \_\_\_\_\_

**E. Categories of Sensitive Personal Information.**

*[Check all that apply.]*

- ☐ Social Security number, driver's license, state ID, passport
- ☐ Account log-in credentials, financial account information
- ☐ Precise geolocation
- ☐ Racial or ethnic origin, religious or philosophical beliefs, union membership
- ☐ Genetic data
- ☐ Biometric information for unique identification
- ☐ Medical Information as defined in Civil Code § 56.05(j) (subject to CMIA; CMIA contractual obligations under § 5.3 apply)
- ☐ Protected Health Information as defined in 45 CFR § 160.103 (subject to HIPAA; Business Associate Agreement required per § 5.3(b))
- ☐ Disability-related information Processed in connection with disability retirement applications under Government Code § 31720 et seq.
- ☐ Personal information concerning sex life or sexual orientation
- ☐ Contents of mail, email, and text messages not directed to Contractor
- ☐ None

**F. Frequency and Type of Processing.**

Frequency: ☐ Continuous ☐ Periodic ☐ One-time ☐ Other: \_\_\_\_\_

Type of Processing: \_\_\_\_\_

**G. Approved Hosting Locations.**

All Processing shall occur within the United States. Approved data centers/regions:

\_\_\_\_\_

**H. Approved Subcontractors.**

*[List Subcontractor name, role, location of processing, and description of services. Add rows as needed.]*

1. \_\_\_\_\_
2. \_\_\_\_\_
3. \_\_\_\_\_

**I. Automated Decisionmaking Technology (ADMT).**

- ☐ No ADMT will be used in connection with the Services.
- ☐ ADMT will be used as described below. For each ADMT, provide: name; provider; intended use; categories of inputs and outputs; whether the ADMT contributes to a Significant Decision; logic and intended outcomes.

ADMT description: \_\_\_\_\_

**J. Retention Schedule.**

Personal Information shall be retained only for the period reasonably necessary to perform the Permitted Purposes, and in no event longer than:

\_\_\_\_\_

(plus any minimum retention period required by applicable law, identified below)

Legal retention obligations: \_\_\_\_\_

**K. Designated Contacts.**

OCERS Privacy/Compliance Contact: \_\_\_\_\_

Contractor Privacy Officer / DPO equivalent: \_\_\_\_\_

Contractor Cybersecurity Audit Contact (per Section 6.3): \_\_\_\_\_

Contractor Security Incident Contact (24x7): \_\_\_\_\_