DATA PROCESSING AGREEMENT

(DPA)

Enterprise SaaS Data Processing Agreement

Multi-Jurisdictional • Multi-Regulatory Compliance

GDPR • UK GDPR • FADP • CCPA/CPRA • VCDPA • CPA • CTDPA • UCPA • TDPSA • OCPA
MCDPA • ICDPA • INCDPA • TIPA • DPDPA • NHPA • NJDPA • NDPA • MODPA • MCDPA-MN • KCDPA • RIDTPPA
LGPD • PIPEDA • HIPAA (BAA Reference) • PCI DSS • COPPA • BIPA • GLBA • FERPA

Version: 1.0 | **Last Updated:** April 12, 2026

Phoenix Holdings LLC

https://dealmatrixcrm.com/legal/dpa

IMPORTANT — HOW THIS DPA APPLIES

This Data Processing Agreement ("Agreement" or "DPA") is incorporated by reference into, and forms an integral part of, the Terms of Service, Master Subscription Agreement, Order Form, or other written or electronic agreement (the "Principal Agreement") between the entity identified as the customer in the Principal Agreement ("Controller," "Customer," or "You") and Phoenix Holdings LLC, an Illinois limited liability company ("Processor," "Provider," or "We").

This DPA becomes legally binding upon the earliest of: (a) the Customer's execution of a Principal Agreement that references this DPA; (b) the Customer's electronic acceptance via click-through, check-box, or digital signature; or (c) the Customer's continued use of the Services after this DPA has been published at the Processor's designated URL (the "Effective Date"). Where the Customer enters this DPA on behalf of an entity, the individual accepting represents and warrants that they have authority to bind that entity. If the individual lacks such authority, they must not accept.

This DPA applies only where the Processor Processes Personal Data on behalf of the Customer in connection with the Services. To the extent the Processor Processes Personal Data as an independent Controller (e.g., account registration data, billing data, usage telemetry for service improvement, or aggregated analytics), such Processing is governed by the Processor's Privacy Policy, not this DPA. The Processor's Privacy Policy is available at https://dealmatrixcrm.com/privacy.

Version: 1.0 | **Last Updated:** April 12, 2026 | **Effective Date:** As defined above

Current version always available at: https://dealmatrixcrm.com/legal/dpa

RECITALS

WHEREAS, the Controller has engaged the Processor to provide certain software-as-a-service ("SaaS") services under the Principal Agreement;

WHEREAS, in providing the Services, the Processor will Process Personal Data on behalf of the Controller;

WHEREAS, the Parties wish to establish terms governing such Processing in compliance with all Applicable Data Protection Laws, including the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"); the UK Data Protection Act 2018 and UK GDPR; the Swiss Federal Act on Data Protection ("FADP"); the California Consumer Privacy Act and California Privacy Rights Act ("CPA/CPRA"); the Virginia Consumer Data Protection Act ("VCDPA"); the Colorado Privacy Act ("CPA-CO"); the Connecticut Data Privacy Act ("CTDPA"); the Utah Consumer Privacy Act ("UCPA"); the Texas Data Privacy and Security Act ("TDPSA"); the Oregon Consumer Privacy Act ("OCPA"); the Montana Consumer Data Privacy Act ("MCDPA"); the Iowa Consumer Data Protection Act ("ICDPA"); the Indiana Consumer Data Protection Act ("INCDPA"); the Tennessee Information Protection Act ("TIPA"); the Delaware Personal Data Privacy Act ("DPDPA"); the New Hampshire Privacy Act ("NHPA"); the New Jersey Data Privacy Act ("NJDPA"); the Nebraska Data Privacy Act ("NDPA"); the Maryland Online Data Privacy Act ("MODPA"); the Minnesota Consumer Data Privacy Act ("MCDPA-MN"); the Kentucky Consumer Data Protection Act ("KCDPA"); the Rhode Island Data Transparency and Privacy Protection Act ("RIDTPPA"); the Brazilian General Data Protection Law ("LGPD"); the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"); and all other applicable data protection or privacy legislation;

NOW, THEREFORE, the Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

Capitalized terms shall have the meanings defined below. Undefined terms carry the meanings set forth in the Principal Agreement or Applicable Data Protection Laws.

Term	Definition
Applicable Data Protection Laws	All laws and regulations applicable to the Processing of Personal Data under this Agreement, as enumerated in the Recitals, and any implementing regulations, guidance, or successor legislation.
Authorized Persons	Employees, agents, consultants, and contractors of the Processor or a Sub-processor who are authorized to Process Personal Data and bound by confidentiality obligations per Section 3.3.
Controller	The Party that determines the purposes and means of Processing, as identified in the Principal Agreement.
Customer Data	All electronic data, text, messages, images, files, or other content submitted by or on behalf of the Controller or its authorized users to the

	Services, including Personal Data contained therein. Customer Data does not include Service-Generated Data.
Data Protection Officer (DPO)	The individual designated by either Party to oversee compliance with Applicable Data Protection Laws, as specified in Schedule 1.
Data Subject	An identified or identifiable natural person to whom Personal Data relates.
De-identified / Anonymized Data	Data processed so it can no longer be attributed to a specific Data Subject without additional information (pseudonymized) or from which all personal identifiers have been irreversibly removed (anonymized) such that it no longer constitutes Personal Data.
EEA	The European Economic Area (EU Member States plus Iceland, Liechtenstein, and Norway).
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council.
Government Access Request	Any request, demand, order, subpoena, warrant, or directive from any law enforcement, judicial, governmental, regulatory, legislative, intelligence, or national security authority for access to or disclosure of Personal Data, whether compulsory or voluntary.
Incident Severity Classification	The risk-based categorization of Personal Data Breaches: Critical (mass exfiltration, ransomware with data loss, or breach of unencrypted special category data); High (unauthorized access to significant volumes of Personal Data); Medium (unauthorized access to limited Personal Data with low likelihood of harm); Low (security event with no confirmed data compromise).
Personal Data	Any information relating to an identified or identifiable natural person Processed by the Processor on behalf of the Controller in connection with the Services. “Personal Data” includes “personal information” as defined in the CCPA/CPRA, “personal data” as defined in the VCDPA, CPA-CO, CTDPA, and other U.S. State Privacy Laws, and equivalent concepts under all Applicable Data Protection Laws.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data, including any “security incident,” “breach of security,” or equivalent concept under Applicable Data Protection Laws.
Processing / Process	Any operation on Personal Data, whether automated or not, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, and destruction.
Processor	The Party that Processes Personal Data on behalf of the Controller, as identified in the Principal Agreement.
Restricted Transfer	A transfer of Personal Data to a country outside the EEA, UK, or Switzerland not covered by an adequacy decision.

SCCs	The Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914, as amended, supplemented, or replaced.
Service-Generated Data	Data generated by the Processor through the operation of the Services that is derived from, but does not directly reveal, Personal Data, including aggregated usage statistics, performance metrics, system logs, error reports, and telemetry data. Service-Generated Data does not include Customer Data.
Services	The SaaS services and related professional, support, and implementation services provided under the Principal Agreement.
Sub-processor	Any third party (excluding the Processor's employees acting under its direct authority) engaged by the Processor or a Sub-processor to Process Personal Data on behalf of the Controller.
Supervisory Authority	An independent public authority established under Article 51 GDPR, the UK ICO, the Swiss FDPIC, the California Privacy Protection Agency (CPPA), State Attorneys General with enforcement authority under U.S. State Privacy Laws, the ANPD (Brazil), the OPC (Canada), or any equivalent regulatory authority.
Technical and Organizational Measures (TOMs)	The administrative, technical, physical, and organizational security measures described in Schedule 2, implemented to protect Personal Data against unauthorized or unlawful Processing and against accidental loss, destruction, or damage.
Transfer Impact Assessment (TIA)	A documented assessment of the data protection laws and practices of a destination country to determine whether they provide an essentially equivalent level of protection and to identify any required supplementary measures.
U.S. State Privacy Laws	Collectively, the CCPA/CPRA, VCDPA, CPA-CO, CTDPA, UCPA, TDPSA, OCPA, MCDPA, ICDPA, INCDPA, TIPA, DPDPA, NHPA, NJDPA, NDPA, MODPA, MCDPA-MN, KCDPA, RIDTPPA, and any future U.S. state comprehensive privacy legislation that becomes applicable to the Processing.

1.2 Interpretation. (a) "Include" or "including" means "including without limitation." (b) References to legislation include amendments, re-enactments, implementing regulations, and successors. (c) "Writing" includes electronic communications. (d) Headings are for convenience only. (e) References to GDPR articles include equivalent provisions under all Applicable Data Protection Laws, mutatis mutandis. (f) The word "shall" denotes a mandatory obligation; "may" denotes a discretionary right. (g) "Business day" means a day other than a Saturday, Sunday, or public holiday in the jurisdiction of the Party required to act.

1.3 Customer Data Ownership. As between the Parties, the Controller retains all right, title, and interest in Customer Data. Nothing in this Agreement or the Principal Agreement grants the Processor any right, title, or interest in Customer Data except the limited rights necessary to perform the Services.

2. SCOPE, PURPOSE, AND RELATIONSHIP OF THE PARTIES

2.1 This Agreement applies to all Processing of Personal Data by the Processor on behalf of the Controller in connection with the Services.

2.2 The subject matter, nature, purpose, duration, types of Personal Data, and categories of Data Subjects are described in Schedule 1 (Details of Processing).

2.3 The duration of Processing is coterminous with the Principal Agreement, unless otherwise specified in Schedule 1 or required by law.

2.4 Order of Precedence. Conflicts are resolved: (i) SCCs (where applicable) prevail over this DPA; (ii) this DPA prevails over the Principal Agreement regarding Processing of Personal Data; (iii) the Principal Agreement governs all other matters.

2.5 Roles. The Controller is the “controller” (or “business” under CCPA) and the Processor is the “processor” (or “service provider” under CCPA) with respect to Customer Data. Where the Processor Processes Service-Generated Data for its own legitimate purposes (service improvement, security, aggregate analytics), the Processor acts as an independent controller for that limited Processing, subject to its Privacy Policy.

2.6 No Joint Controller Relationship. Nothing in this Agreement creates a joint controller relationship unless expressly documented in a separate joint controller agreement executed by both Parties.

2.7 Multi-Tenant Architecture. The Processor shall implement logical and/or physical isolation of each Customer’s data within its multi-tenant infrastructure sufficient to prevent unauthorized cross-tenant access. The Processor shall maintain access controls, authentication boundaries, and encryption practices that ensure Customer Data is not accessible to other tenants of the Services.

3. PROCESSOR OBLIGATIONS

3.1 Documented Instructions. The Processor shall Process Personal Data only on documented instructions from the Controller (which include this Agreement and the Principal Agreement), including regarding international transfers, unless required by applicable law. If so required, the Processor shall inform the Controller before Processing, unless prohibited by law on important public interest grounds.

3.2 Article 28 Compliance. The Processor warrants that it satisfies each requirement of Article 28 GDPR and equivalent provisions of all other Applicable Data Protection Laws.

3.3 Confidentiality. The Processor shall ensure all Authorized Persons: (a) are bound by written confidentiality obligations (contractual or statutory) no less protective than this Agreement; (b) Process Personal Data only as necessary for the Services; (c) receive onboarding and annual data protection and security training. These obligations survive termination of engagement.

3.4 Prohibited Processing. The Processor shall not:

(a) Sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate Personal Data for monetary or other valuable consideration;

(b) Share Personal Data for cross-context behavioral advertising (as defined in CCPA/CPRA §1798.140(ah));

(c) Retain, use, or disclose Personal Data for any purpose other than performing the Services, including any commercial purpose outside the direct business relationship;

(d) Combine Personal Data from the Controller with Personal Data received from or on behalf of third parties, or collected from the Processor's own consumer interactions, except as expressly permitted by Applicable Data Protection Laws;

(e) Use Personal Data for profiling, targeted advertising, automated decision-making (except as an integral feature of the Services documented in the Principal Agreement), or cross-context behavioral advertising;

(f) Use Personal Data to train, develop, improve, or fine-tune any machine learning, artificial intelligence, or algorithmic model (whether general or specific) without the Controller's prior, specific, written consent;

(g) Process Personal Data in a manner that would cause the Controller to be in violation of Applicable Data Protection Laws;

(h) Disclose Personal Data to any governmental authority except as compelled by valid legal process, subject to Section 11; or

(i) Degrade the Services or discriminate against Data Subjects who exercise privacy rights, directly or indirectly.

3.5 Instruction Review. If an instruction infringes Applicable Data Protection Laws in the Processor's reasonable opinion, the Processor shall immediately notify the Controller and may suspend the relevant Processing until the Controller confirms or modifies the instruction. The Processor is not required to independently assess instruction legality but shall act in good faith.

3.6 Data Protection Officer. The Processor shall appoint and maintain a DPO (or equivalent privacy officer). Contact details shall be provided on request and updated promptly.

3.7 Records of Processing. The Processor shall maintain complete records of Processing activities per Article 30(2) GDPR, available to the Controller and Supervisory Authorities on request.

3.8 Certification. The Processor hereby certifies that it understands and will comply with the restrictions set forth in this Section 3.

4. CONTROLLER OBLIGATIONS AND WARRANTIES

4.1 The Controller represents, warrants, and covenants that:

(j) It has complied and will comply with all Applicable Data Protection Laws regarding collection, use, and transfer of Personal Data;

(k) It has established a lawful basis for Processing (Article 6 GDPR or equivalent), provided adequate notice, and obtained all consents and authorizations required;

(l) Its instructions shall at all times comply with Applicable Data Protection Laws;

(m) It has conducted and will maintain required DPIAs;

(n) It has authority to transfer Personal Data to the Processor;

(o) It will not submit to the Services any Personal Data that the Processor is not equipped to protect (e.g., protected health information requiring HIPAA BAA compliance, unless a BAA is separately executed per Schedule 6); and

(p) It will cooperate with the Processor in addressing Data Subject requests, Supervisory Authority inquiries, and DPIAs.

4.2 The Controller is solely responsible for the accuracy, quality, and legality of Personal Data and the lawfulness of its instructions.

4.3 The Controller shall implement appropriate security within elements it configures or controls, including user access management, authentication settings, data classification, and API key management.

4.4 The Controller acknowledges that the Processor's ability to comply with certain obligations may be contingent upon the Controller's timely performance of its obligations under this Agreement.

5. DATA SUBJECT RIGHTS

5.1 The Processor shall assist the Controller, by appropriate technical and organizational measures, in fulfilling Data Subject rights requests under Applicable Data Protection Laws, including:

(q) Access (Art. 15 GDPR; CCPA §1798.100; equivalent state law provisions);

(r) Rectification / Correction (Art. 16 GDPR; CPRA §1798.106);

(s) Erasure / Deletion (Art. 17 GDPR; CCPA §1798.105);

(t) Restriction of Processing (Art. 18 GDPR);

(u) Data Portability (Art. 20 GDPR);

(v) Objection (Art. 21 GDPR);

(w) Automated Decision-Making/Profiling Opt-Out (Art. 22 GDPR);

(x) Opt-Out of Sale/Sharing (CCPA/CPRA §1798.120), including recognition and honoring of Global Privacy Control (GPC) signals and other universal opt-out mechanisms as required by law;

(y) Limit Use of Sensitive Personal Information (CPRA §1798.121);

(z) Non-Discrimination for exercising privacy rights (CCPA §1798.125); and

(aa) Equivalent rights under all other U.S. State Privacy Laws and international data protection statutes.

5.2 The Processor shall notify the Controller of any Data Subject request within three (3) business days. The Processor shall not respond except to acknowledge receipt and direct the Data Subject to the Controller, unless authorized in writing.

5.3 The Processor shall maintain self-service technical capabilities enabling the Controller to search, export, rectify, restrict, and delete Personal Data within statutory timeframes, at no additional cost for standard-volume requests.

5.3.1 Excessive or Manifestly Unfounded Requests. Where Data Subject requests forwarded by the Controller are manifestly unfounded, excessive, or repetitive (as assessed in accordance with Article 12(5) GDPR or equivalent provisions), or where the Controller requests assistance beyond what is available through the Processor's standard self-service tools, the Processor may charge a reasonable fee based on administrative costs. The Processor shall notify the Controller of such fees in advance and shall not charge fees that would prevent the Controller from complying with Applicable Data Protection Laws.

5.4 CCPA Verifiable Consumer Requests. If the Processor receives a verifiable consumer request directly from a California consumer, the Processor shall either act on behalf of the Controller per CCPA implementing regulations or promptly inform the Controller and await instructions.

5.5 Universal Opt-Out Signals. The Processor shall, within the Services, honor opt-out preference signals (including GPC) as required by the CCPA/CPRA, CPA-CO, CTDPA, MODPA, and any other jurisdiction mandating recognition of such signals.

6. SUB-PROCESSORS

6.1 General Authorization. The Controller grants general written authorization to engage Sub-processors, subject to this Section 6. The current Sub-processor list is in Schedule 3 and published at https://dealmatrixcrm.com/legal/sub-processors. The Controller may subscribe to updates via email, RSS, or webhook at https://dealmatrixcrm.com/legal/sub-processors#subscribe.

6.2 Notification. The Processor shall notify the Controller in writing (email or subscription mechanism) of any intended addition, replacement, or material change to Sub-processors at least thirty (30) calendar days before engagement (the “Objection Period”). Notification shall include: Sub-processor name, legal entity, registered address, country of Processing, description of activities, applicable transfer mechanism, and security certifications held.

6.2.1 Emergency Sub-processor Engagement. Notwithstanding Section 6.2, the Processor may engage a replacement or new Sub-processor immediately, without prior notice, where such engagement is reasonably necessary to: (a) address an active security vulnerability, data breach, or imminent threat to the security of Personal Data; (b) respond to a material service outage or failure of an existing Sub-processor that impacts the availability of the Services; or (c) comply with a binding legal or regulatory requirement. In such cases, the Processor shall: (i) notify the Controller as soon as practicable and in no event later than five (5) business days after engagement; (ii) provide the same information required under Section 6.2; (iii) ensure the emergency Sub-processor is bound by obligations no less protective than this Agreement per Section 6.4; and (iv) grant the Controller a retroactive fifteen (15) calendar day objection period following notification, with the same objection rights and remedies set forth in Section 6.3.

6.3 Objection. The Controller may object on reasonable data protection grounds within the Objection Period by written notice stating specific concerns. Upon objection: (a) the Processor shall use commercially reasonable efforts to provide an alternative avoiding the objected-to Sub-processor within thirty (30) days; (b) if no alternative is available, either Party may terminate the affected Services (only) upon written notice, with a pro-rata refund of prepaid fees. Termination under this Section is not a breach by either Party.

6.4 Sub-processor Contracts. The Processor shall impose on each Sub-processor written obligations no less protective than this Agreement, including equivalent provisions regarding confidentiality, security, breach notification, data subject rights, international transfers, audit, and return/deletion. Sub-processor contracts shall include flow-down clauses requiring equivalent obligations on any further Sub-processor.

6.5 Full Liability. The Processor remains fully liable for Sub-processor acts and omissions as if they were the Processor’s own.

6.6 Due Diligence. Before engaging any Sub-processor, the Processor shall conduct risk-based due diligence assessing the Sub-processor’s ability to provide sufficient data protection guarantees. Critical and high-risk Sub-processors shall be reassessed at least annually; all others at least biennially.

6.7 Upon request, the Processor shall provide the Controller with a summary of the data protection terms in its Sub-processor agreements (redacted for proprietary terms unrelated to data protection).

7. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

7.1 The Processor shall implement and maintain TOMs ensuring a level of security appropriate to the risk, per Article 32 GDPR, taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of Processing.

7.2 Minimum Security Controls:

(bb) Encryption: AES-256 (or equivalent) at rest; TLS 1.2+ in transit (TLS 1.3 preferred); HSM-backed key management with automated key rotation; encrypted backups with segregated key management; option for customer-managed encryption keys (CMEK/BYOK) where supported by the Service tier.

(cc) Access Controls: RBAC with least-privilege; MFA for all administrative, privileged, and production access; SSO (SAML 2.0/OIDC); SCIM-based automated provisioning/de-provisioning; PAM for infrastructure; quarterly access certifications; session management (timeout, concurrent session limits); IP allowlisting.

(dd) Network Security: Defense-in-depth; segmentation and micro-segmentation; next-gen firewalls with deep packet inspection; IDS/IPS; enterprise DDoS mitigation; WAF with custom rulesets; DNSSEC; VPN/zero-trust for administrative access; egress filtering and data exfiltration detection.

(ee) Application Security: Secure SDLC; OWASP Top 10 and SANS Top 25 mitigation; SAST, DAST, and SCA in CI/CD; peer code review with security focus; dependency scanning with automated alerting; input validation and output encoding; CSP and security headers; API rate limiting, authentication, and authorization; container image scanning.

(ff) Monitoring and Logging: 24/7 SOC (internal or managed); SIEM with correlation and anomaly detection; centralized logging (12-month minimum retention, 24 months for security events); database activity monitoring; file integrity monitoring; UEBA; CSPM; real-time alerting with defined escalation procedures.

(gg) Vulnerability Management: Continuous automated scanning; annual independent penetration testing (black box, gray box, and application-layer); responsible disclosure/bug bounty program; risk-rated patch management (critical: 24h, high: 7 days, medium: 30 days, low: 90 days); CIS Benchmark hardening.

(hh) Physical Security: Tier III+ data centers; SOC 2 Type II and/or ISO 27001 certified facilities; multi-factor physical access (badge + biometric); 24/7 on-site security and CCTV (90-day retention); mantrap entry; environmental controls (fire suppression, redundant HVAC, UPS, generators); visitor management with escorts.

(ii) Business Continuity / DR: Board-approved BCP/DR plans; annual testing with documented results; geographically distributed redundancy (active-active or active-

passive); defined RTO/RPO per service tier; automated failover; backup integrity testing; pandemic and supply-chain contingency planning.

(jj) Personnel Security: Background checks (criminal, education, employment verification); onboarding and annual security awareness training with phishing simulations; role-specific privileged-user training; acceptable use, clean desk, and screen lock policies; NDA/confidentiality agreements; disciplinary procedures; immediate access revocation on termination; exit interviews.

(kk) Data Management: Classification framework (public, internal, confidential, restricted); pseudonymization and tokenization; data minimization by design and default; DLP (endpoint, network, cloud); secure deletion per NIST SP 800-88; data inventory and mapping; privacy-by-design embedded in development; data masking in non-production environments.

(ll) Incident Response: NIST SP 800-61 aligned IR plan; designated 24/7 on-call IR team; semi-annual tabletop exercises; external forensics retainer; automated containment playbooks; post-incident review with root-cause analysis; pre-drafted communication templates; lessons-learned tracking.

(mm) Third-Party / Supply Chain: Risk-tiered vendor assessment (SIG/CAIQ); contractual security and privacy requirements; annual reassessment of critical vendors; right-to-audit clauses; supply chain integrity verification; fourth-party risk monitoring; software bill of materials (SBOM) for critical dependencies.

7.3 The Processor shall test, assess, and evaluate TOMs effectiveness at least annually and update as needed. Updates shall not materially decrease the overall protection level. The Processor shall notify the Controller of any material changes.

7.4 Detailed TOMs are described in Schedule 2. The Processor shall respond to the Controller’s reasonable security questionnaires (e.g., SIG, CAIQ, VSAQ) within fifteen (15) business days.

7.5 Customer-Managed Keys. Where the Controller’s service tier supports CMEK/BYOK, the Controller may manage its own encryption keys. In such cases, the Processor shall not have the ability to decrypt Customer Data without the Controller’s key, and the Controller assumes responsibility for key management.

8. PERSONAL DATA BREACH NOTIFICATION AND RESPONSE

8.1 Initial Notification. The Processor shall notify the Controller of any confirmed or reasonably suspected Personal Data Breach without undue delay and no later than:

(nn) Critical or High severity: thirty-six (36) hours after becoming aware;

(oo) Medium severity: forty-eight (48) hours after becoming aware;

(pp) Low severity: seventy-two (72) hours after becoming aware.

Notification shall be by email to the Controller's designated data protection contact. Critical and High severity breaches shall additionally be notified by telephone.

8.2 Content. The initial notification shall include (to the extent reasonably available):

(qq) Date/time of discovery and estimated date/time of occurrence;

(rr) Incident Severity Classification and basis for classification;

(ss) Nature of the breach, including categories and approximate number of Data Subjects and records affected;

(tt) Types of Personal Data involved (including whether special categories or sensitive data are implicated);

(uu) Name and contact details of the Processor's DPO or incident coordinator;

(vv) Likely consequences of the breach;

(ww) Measures taken or proposed to contain, mitigate, and remediate;

(xx) Preliminary root-cause analysis;

(yy) Assessment of whether the breach is likely to result in a risk or high risk to Data Subjects; and

(zz) Jurisdictions likely affected (for breach notification law analysis).

8.3 Supplemental Reporting. Supplemental reports at intervals of no greater than twenty-four (24) hours until investigation concludes. A final written incident report within ten (10) business days of containment, including root cause, scope of impact, remediation steps, and preventive measures.

8.4 Cooperation. The Processor shall: (a) cooperate fully in investigation, mitigation, and remediation; (b) immediately contain the breach; (c) preserve forensic evidence for a minimum of three (3) years; (d) implement measures to prevent recurrence; (e) conduct post-incident review and share findings; (f) at the Controller's request, engage a mutually agreed independent forensic investigator at the Processor's expense if the breach resulted from the Processor's act or omission.

8.5 Regulatory and Data Subject Notification. The Processor shall not notify third parties (Data Subjects, Supervisory Authorities, State Attorneys General, media, credit monitoring agencies) without the Controller's prior written consent, unless legally compelled. If compelled, the Processor shall provide maximum practicable advance notice and coordinate content and timing

with the Controller. The Processor shall assist the Controller in preparing notifications and shall bear the reasonable costs of notification (including credit monitoring services) where the breach resulted from the Processor's act or omission.

8.6 State-Specific Breach Notification. The Processor shall assist the Controller in complying with the breach notification timelines of each applicable U.S. state (which range from thirty (30) to ninety (90) days depending on jurisdiction) and shall provide sufficient information for the Controller to assess notification obligations under each applicable state law and to notify State Attorneys General where required.

8.7 Breach Register. The Processor shall maintain a register per Article 33(5) GDPR, documenting facts, effects, severity classification, and remedial actions.

8.8 Sub-processor Breaches. Obligations in this Section 8 apply regardless of whether the breach occurs at the Processor or any Sub-processor. The Processor shall require Sub-processors to notify the Processor within twenty-four (24) hours of becoming aware of a breach.

8.9 No Admission. The Processor's notification of a Personal Data Breach, investigation of a suspected breach, or implementation of remedial measures shall not be construed as an acknowledgment or admission by the Processor of any fault, liability, or wrongdoing. The Processor's obligation to notify is a compliance measure, not an admission of causation.

9. DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION

9.1 The Processor shall provide reasonable assistance with DPIAs and prior consultation with Supervisory Authorities, taking into account the nature of Processing and available information.

9.2 Assistance includes: (a) detailed descriptions of Processing, data flows, and TOMs; (b) risk identification and assessment; (c) identification of mitigating measures; (d) technical architecture and security documentation; and (e) cooperation with Supervisory Authority inquiries.

9.3 The Processor shall notify the Controller if changes to the Services, Processing, or regulatory environment are likely to require a new or updated DPIA.

9.4 Where U.S. State Privacy Laws require data protection assessments (e.g., VCDPA §59.1-580; CPA-CO §6-1-1309; CTDPA §42-520; TDPSA; MODPA), the Processor shall cooperate and provide information equivalent to that required for a GDPR DPIA.

10. INTERNATIONAL DATA TRANSFERS

10.1 Transfer Restriction. The Processor shall not make any Restricted Transfer unless a valid transfer mechanism is in place:

(aaa) Adequacy decision (European Commission, UK Secretary of State, or Swiss FDPIC);

(bbb) SCCs (Implementing Decision 2021/914), supplemented by a TIA;

(ccc) Binding Corporate Rules approved by the competent Supervisory Authority;

(ddd) UK IDTA or UK Addendum to the EU SCCs;

(eee) Approved certification (EU-U.S. DPF, UK Extension, Swiss-U.S. DPF) with binding enforceable commitments; or

(fff) Any other legally valid mechanism.

10.2 SCCs Configuration. Where SCCs apply: Module 2 (C2P) and/or Module 3 (P2P); Clause 7 (Docking) included; Clause 9 Option 2 (general authorization, 30-day objection); Clause 11 optional redress language included; Clause 13(a): competent SA of Controller's establishment; Clause 17 Option 1: law of Controller's EU establishment (or Ireland if none); Clause 18(b): courts of that jurisdiction. SCCs incorporated as Annex A. SCCs prevail over this DPA in case of conflict.

10.3 Transfer Impact Assessments. The Processor shall conduct, document, and maintain a TIA for each Restricted Transfer, evaluating: (a) destination country laws (including government surveillance and access laws, with reference to EDPB Recommendations 01/2020); (b) specific transfer circumstances; (c) supplementary measures; (d) overall risk conclusion. TIAs updated at least annually or upon material change. Available to Controller and Supervisory Authorities on request.

10.4 Supplementary Measures. Where a TIA identifies deficiencies: additional encryption (including in-use encryption where feasible), pseudonymization, key management outside the destination country, access restrictions, data localization, split processing, or contractual commitments to challenge government access using all available legal remedies and to notify the Controller (subject to Section 11).

10.5 The Processor shall promptly notify the Controller of any change materially affecting the validity of a transfer mechanism or TIA.

10.6 See Schedule 4 for detailed transfer mechanism configurations.

11. GOVERNMENT ACCESS REQUESTS AND TRANSPARENCY

11.1 Upon receipt of a Government Access Request, the Processor shall:

(ggg) Promptly notify the Controller before any disclosure, unless legally prohibited;

(hhh) Redirect the authority to the Controller where permissible;

(iii) Scrutinize the legal basis and challenge any request that is unlawful, overbroad, or disproportionate, using all available legal mechanisms including appeals;

(jjj) Disclose only the minimum data legally compelled;

(kkk) Provide the data in encrypted form if possible; and

(lll) Document and retain records of all requests and responses.

11.2 If legally prohibited from notifying the Controller, the Processor shall: (a) seek a waiver or modification of the prohibition; (b) disclose maximum permissible information as soon as legally allowed; and (c) provide an annual summary of the number and types of prohibited requests (to the extent legally permissible).

11.3 Warranties. As of the Effective Date, the Processor warrants: (a) it has not received any request requiring bulk or indiscriminate access to Personal Data; (b) it has no knowledge of any law preventing it from fulfilling this Agreement; (c) it has not voluntarily provided Personal Data to any government authority outside documented lawful process; and (d) it has not created, and will not create, any “back door” or equivalent mechanism for government access. The Processor shall promptly notify the Controller if any of these warranties ceases to be true.

11.4 Transparency Report. The Processor shall publish or make available an annual transparency report summarizing request volumes and types (to the extent permitted by law).

11.5 Mutual Legal Assistance. Where a Government Access Request is made under a mutual legal assistance treaty (MLAT) or equivalent mechanism, the Processor shall cooperate with the Controller in assessing whether the request complies with applicable procedures and inform the Controller of the request’s status.

12. AUDIT RIGHTS AND COMPLIANCE VERIFICATION

12.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with this Agreement and Applicable Data Protection Laws, and shall allow and contribute to audits, including inspections, by the Controller or its mandated qualified independent auditor (subject to reasonable confidentiality obligations not to disclose other customers' data).

12.2 Audit Schedule. One (1) comprehensive audit per twelve-month period upon thirty (30) calendar days' notice, during business hours. Additional audits permitted: (a) if required by a Supervisory Authority; (b) following a Personal Data Breach; (c) upon reasonable suspicion of non-compliance; or (d) as required under the SCCs.

12.3 Audit Costs. The Controller bears costs of routine annual audits. The Processor bears costs of audits triggered by Processor breach or non-compliance, including the cost of any independent forensic investigation.

12.4 Certifications and Reports. The Processor shall maintain and provide upon request:

(mmm) SOC 2 Type II report (annual);

(nnn) ISO/IEC 27001 certification;

(ooo) ISO/IEC 27701 certification (if applicable);

(ppp) ISO/IEC 27018 certification (if applicable, for cloud privacy);

(qqq) Annual penetration test executive summary;

(rrr) PCI DSS Attestation of Compliance (if payment data is Processed);

(sss) HITRUST CSF certification (if applicable); and

(ttt) Any other relevant certifications.

These reports may satisfy audit requirements where they reasonably cover the audit scope. The Controller may review certifications and reports under NDA.

12.5 Remediation. Non-compliance discovered by audit: (a) written remediation plan within ten (10) business days; (b) remediation evidence within thirty (30) calendar days (or shorter if the nature requires); (c) the Processor bears all remediation costs. Material unremediated non-compliance constitutes a material breach.

12.6 Annual Compliance Attestation. The Processor shall provide an annual written attestation, signed by its CISO or equivalent officer, confirming material compliance with this Agreement.

12.7 Penetration Testing. The Controller may conduct or commission application-layer penetration testing of the Services upon fifteen (15) business days' prior written notice, coordinated with the Processor to minimize service disruption. Results shall be shared with the Processor for remediation.

12.8 Security Questionnaires. The Processor shall respond to the Controller's reasonable security questionnaires (SIG Lite, SIG Full, CAIQ, VSAQ, or equivalent) within fifteen (15) business days of receipt.

12.9 Regulatory Cooperation. Full cooperation with Supervisory Authority investigations; prompt notification to the Controller of any investigation, inquiry, or complaint.

12.10 Audit Limitations. All audits shall: (a) be conducted in a manner that minimizes disruption to the Processor's operations and other customers; (b) comply with the Processor's reasonable security and access policies; (c) not access, view, or compromise the data of any other customer of the Processor; (d) be subject to reasonable confidentiality obligations binding on the Controller and its auditors; and (e) not include penetration testing without prior coordination per Section 12.7. The Controller shall bear responsibility for any damage caused by its auditors during an audit.

12.11 Processor's Right to Suspend. If the Controller is in material breach of this Agreement (including failure to pay fees under the Principal Agreement, submission of data in violation of Section 4.1(f), or issuance of unlawful Processing instructions), the Processor may, after providing thirty (30) calendar days' written notice and opportunity to cure: (a) suspend Processing of Personal Data until the breach is cured; and (b) if the breach remains uncured, terminate this Agreement per Section 20.2. During any suspension, the Processor shall continue to secure Personal Data in its possession but shall not be obligated to perform active Processing. The Processor shall not suspend Processing where doing so would cause the Controller to violate Applicable Data Protection Laws regarding Data Subject rights, unless the suspension is itself required by law.

13. DATA RETENTION, RETURN, AND DELETION

13.1 Upon termination/expiration or the Controller's earlier written request, the Processor shall, at the Controller's election: (a) return all Customer Data in a commonly used, machine-readable, interoperable, and portable format (CSV, JSON, XML, or API-based bulk export); or (b) securely delete all Customer Data (including copies, replicas, backups, logs, caches, indexes, and any derivative data from which Personal Data can be reconstructed) using methods conforming to NIST SP 800-88, and provide a signed certification of destruction specifying data destroyed, methods used, and completion date.

13.2 Timeline. Return or deletion completed within thirty (30) calendar days.

13.3 Legal Retention Exception. Retention permitted only to the extent required by law, provided: (a) continued confidentiality and security; (b) Processing limited to the legally required purpose; (c) deletion upon expiration of the retention period; (d) the Controller is informed of the retention obligation, legal basis, and expected duration; and (e) retained data remains subject to this Agreement.

13.4 Transition Assistance. Ninety (90) calendar day post-termination transition period for data export via self-service tools, at no additional charge. Reasonable Processor cooperation during

this period. All remaining Customer Data securely deleted within thirty (30) days after transition period expiration.

13.5 Backup Handling. Where individual deletion from backup/archival systems is not technically feasible, the Processor shall: (a) isolate and protect data from further Processing; (b) continue applying this Agreement's protections; (c) delete data per standard backup rotation, not exceeding one hundred eighty (180) calendar days; and (d) confirm deletion in writing upon request.

13.6 Service-Generated Data. Upon termination, the Processor shall delete or anonymize all Service-Generated Data that contains or is derived from identifiable Personal Data within ninety (90) calendar days. Truly anonymized aggregate data may be retained in accordance with Section 16.

14. U.S. STATE PRIVACY LAW PROVISIONS

14.1 California (CCPA/CPRA)

(uuu) The Processor is a “Service Provider” under Cal. Civ. Code §1798.140(ag).

(vvv) The Processor shall not sell or share (per §1798.140(ad), (ah)) Personal Data.

(www) The Processor shall not retain, use, or disclose Personal Data for any commercial purpose other than providing the Services or outside the direct business relationship.

(xxx) The Processor shall not combine Personal Data from the Controller with data from other sources, except as permitted by CCPA/CPRA implementing regulations (§7051).

(yyy) The Controller may take reasonable steps to ensure the Processor uses Personal Data consistently with the Controller’s CCPA/CPRA obligations, including monitoring, auditing, and inspection.

(zzz) The Processor shall notify the Controller if it determines it can no longer meet its CCPA/CPRA obligations.

(aaaa) The Processor shall honor GPC signals and other opt-out preference signals per CPRA regulations and CPPA enforcement guidance.

(bbbb) The Processor hereby certifies that it understands and will comply with these restrictions.

14.2 Comprehensive U.S. State Privacy Laws

For each U.S. State Privacy Law listed in the definition of “U.S. State Privacy Laws” that applies to the Processing:

(cccc) The Processor shall act as a “processor” (or equivalent role) under such law;

(dddd) The Processor shall assist the Controller in responding to consumer rights requests within statutory timeframes;

(eeee) The Processor shall cooperate with required data protection assessments;

(ffff) The Processor shall provide appropriate confidentiality, security, and breach notification guarantees;

(gggg) The Processor shall allow and contribute to reasonable assessments by the Controller;

(hhhh) The Processor shall comply with any state-specific requirements regarding sensitive data, biometric data, or children’s data; and

(iiii) The Processor shall not engage in Processing that would cause the Controller to violate any such law.

14.3 Maryland Online Data Privacy Act (MODPA). The Processor specifically acknowledges MODPA's prohibition on the sale of sensitive data and restrictions on targeted advertising using sensitive data, and shall comply with these provisions.

14.4 Future Laws. If any new U.S. state comprehensive privacy legislation becomes applicable during the term, the Processor shall use commercially reasonable efforts to comply with such legislation and shall cooperate with the Controller in doing so.

15. AUTOMATED DECISION-MAKING, AI, AND MACHINE LEARNING

15.1 No Training Without Consent. The Processor shall not use Customer Data (including Personal Data) to train, develop, improve, or fine-tune any AI/ML model without the Controller's prior, specific, written consent specifying scope, purpose, safeguards, and duration.

15.2 Automated Features. If the Services incorporate automated decision-making or profiling: (a) the Processor shall provide meaningful information about the logic, significance, and envisaged consequences; (b) implement safeguards including human intervention, the ability for Data Subjects to contest decisions, and express their point of view; (c) ensure no legal or similarly significant effects without a lawful basis; and (d) maintain documentation sufficient for the Controller to explain such Processing to Data Subjects and Supervisory Authorities.

15.3 AI Transparency. The Processor shall disclose in its documentation which features of the Services use AI/ML, whether such features are enabled by default, and how the Controller may disable them.

15.4 Bias and Fairness. Where the Services use AI/ML to make or assist decisions about Data Subjects, the Processor shall: (a) regularly test for discriminatory outcomes; (b) take appropriate corrective action; and (c) document its fairness and bias assessment processes.

16. DE-IDENTIFIED, ANONYMIZED, AND AGGREGATED DATA

16.1 The Processor may create De-identified or Anonymized Data only for: (a) providing, maintaining, securing, and improving the Services; (b) internal benchmarking and analytics; or (c) purposes expressly permitted in the Principal Agreement.

16.2 Safeguards. The Processor shall: (a) ensure De-identified/Anonymized Data cannot reasonably be re-identified; (b) not attempt re-identification; (c) contractually prohibit downstream recipients from re-identification; (d) implement technical safeguards (k-anonymity, differential privacy, or equivalent where feasible); (e) treat any accidental re-identification as a Personal Data Breach per Section 8; and (f) maintain documentation of de-identification methods.

16.3 Properly de-identified or anonymized data meeting Section 16.2 criteria is excluded from this Agreement. Burden of proof rests with the Processor.

17. CHILDREN'S DATA, SENSITIVE DATA, AND SECTOR-SPECIFIC REQUIREMENTS

17.1 Children's Data. If the Services involve Processing data of children (under 13 per COPPA; under 16 per GDPR Art. 8; or relevant age threshold elsewhere): (a) compliance with COPPA and equivalent laws; (b) heightened security; (c) no profiling, targeted advertising, or secondary use; (d) support for verifiable parental consent; (e) enhanced deletion capability; and (f) compliance with the Children's Online Privacy Protection Rule (16 CFR Part 312).

17.2 Sensitive / Special Category Data. If applicable: (a) enhanced encryption, access controls, and audit logging; (b) Processing limited to Schedule 1 purposes; (c) strict need-to-know access; (d) sector-specific compliance:

(jjjj) HIPAA: If protected health information (PHI) is Processed, a separate Business Associate Agreement (BAA) per Schedule 6 must be executed prior to Processing. This DPA does not constitute a BAA.

(kkkk) PCI DSS: If payment card data is Processed, the Processor shall maintain PCI DSS compliance and provide its Attestation of Compliance (AOC) annually.

(llll) FERPA: If education records are Processed, the Processor shall comply with the Family Educational Rights and Privacy Act.

(mmmm) GLBA: If financial data subject to the Gramm-Leach-Bliley Act is Processed, the Processor shall maintain an information security program per the FTC Safeguards Rule.

17.3 Biometric Data. Where the Services Process biometric identifiers or biometric information (as defined under Illinois BIPA, Texas CUBI, Washington, or equivalent state law), the Processor shall: (a) not sell, lease, or profit from such data; (b) store, transmit, and protect using reasonable security; (c) retain only as long as necessary for the stated purpose; and (d) permanently destroy upon achieving the purpose or within three (3) years of last interaction, whichever is sooner.

18. DATA LOCALIZATION AND STORAGE

18.1 The Processor shall store and Process Personal Data in the geographic regions specified in Schedule 1 or the Principal Agreement and shall not change locations without prior written notice and compliance with Section 10.

18.2 Where the Controller designates a region for data residency, primary storage, all active Processing, and backups shall remain within that region. Transient processing outside the region (CDN delivery, failover) is permitted only if: (a) disclosed; (b) appropriate transfer mechanisms are in place; and (c) data is encrypted in transit and at rest.

18.3 Data Sovereignty. The Processor shall not Process or store Personal Data in any jurisdiction subject to comprehensive sanctions by the U.S. (OFAC SDN List), EU, or UK without the Controller’s prior written consent.

19. LIABILITY, INDEMNIFICATION, AND INSURANCE

19.1 GDPR Liability. Each Party is liable per Articles 82-83 GDPR, Article 43 UK GDPR, and equivalent provisions.

19.2 Limitation of Liability

19.2.1 General Cap. EXCEPT FOR THE CARVE-OUTS IN SECTION 19.2.3, EACH PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR ANY OTHER LEGAL THEORY, SHALL NOT EXCEED THE GREATER OF: (A) THE TOTAL FEES PAID AND PAYABLE BY THE CONTROLLER TO THE PROCESSOR UNDER THE PRINCIPAL AGREEMENT DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM; OR (B) $100,000 (ONE HUNDRED THOUSAND U.S. DOLLARS).

19.2.2 Exclusion of Consequential Damages. EXCEPT FOR THE CARVE-OUTS IN SECTION 19.2.3, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOSS OF PROFITS, REVENUE, GOODWILL, BUSINESS OPPORTUNITY, DATA (OTHER THAN PERSONAL DATA), OR ANTICIPATED SAVINGS, REGARDLESS OF WHETHER SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF THE LEGAL THEORY UPON WHICH THE CLAIM IS BASED.

19.2.3 Super Cap / Carve-Outs. The following are not subject to the limitations in Sections 19.2.1 and 19.2.2 but are instead subject to a separate aggregate cap equal to two times (2x) the amount in Section 19.2.1(A) (the "Super Cap"): (a) the Processor's indemnification obligations under Section 19.3; (b) either Party's breach of confidentiality (Section 21); (c) the Processor's unauthorized Processing or use of Personal Data for its own purposes in violation of Section 3.4; and (d) the Processor's regulatory fine reimbursement obligations under Section 19.6. The following are not subject to any cap: (i) either Party's liability for fraud, willful misconduct, or gross negligence; (ii) either Party's liability that cannot be limited by applicable law (including mandatory GDPR liability under Article 82); and (iii) either Party's obligation to pay fees owed under the Principal Agreement.

19.3 Indemnification

19.3.1 Processor Indemnification. The Processor shall indemnify, defend, and hold harmless the Controller and its officers, directors, employees, agents, successors, and assigns from all third-party claims, damages, losses, fines, penalties, costs, and expenses (including reasonable attorneys' fees) arising from: (a) Processor's material breach of this Agreement; (b) Processor's violation of Applicable Data Protection Laws attributable to the Processor's acts or omissions (and not resulting from the Controller's instructions or breach); (c) Processor's gross negligence or willful misconduct in Processing Personal Data; (d) Sub-processor acts or omissions per Section 6.5; or (e) breach of the prohibited Processing provisions (Section 3.4).

19.3.2 Controller Indemnification. The Controller shall indemnify, defend, and hold harmless the Processor and its officers, directors, employees, agents, successors, and assigns from all third-party claims, damages, losses, fines, penalties, costs, and expenses (including reasonable attorneys' fees) arising from: (a) Controller's breach of this Agreement, including breach of the warranties in Section 4; (b) Controller's violation of Applicable Data Protection Laws; (c) unlawful, inaccurate, or unauthorized Processing instructions provided by the Controller; (d) the Controller's failure to obtain required consents, provide required notices, or establish a lawful basis for Processing; (e) any claim by a Data Subject arising from the Controller's collection, use, or disclosure of Personal Data prior to or independent of the Services; or (f) any Personal Data submitted to the Services in violation of Section 4.1(f) (e.g., PHI without a BAA, data the Services are not equipped to protect).

19.3.3 Indemnification Procedures. The indemnified Party shall: (a) promptly notify the indemnifying Party in writing of any claim (provided that failure to provide prompt notice shall not relieve the indemnifying Party except to the extent materially prejudiced); (b) grant the indemnifying Party sole control of the defense and settlement of such claim (provided that the indemnifying Party shall not settle any claim without the indemnified Party's prior written consent if the settlement imposes any obligation on, or requires any admission by, the indemnified Party); and (c) provide reasonable cooperation at the indemnifying Party's expense. The indemnified Party may participate in the defense with its own counsel at its own expense.

19.4 Regulatory Fines

19.4.1 Where a regulatory fine or penalty is imposed on the Controller resulting directly and solely from the Processor's breach of this Agreement or Applicable Data Protection Laws (and not resulting from the Controller's instructions, acts, or omissions), the Processor shall reimburse such fine to the extent: (a) it is finally determined to be attributable to the Processor's breach by a court of competent jurisdiction or by mutual written agreement; (b) the Controller has used reasonable efforts to mitigate the fine; and (c) the Controller provided the Processor with prompt notice and reasonable opportunity to participate in any proceedings related to the fine. Reimbursement under this Section is subject to the Super Cap in Section 19.2.3.

19.4.2 Where a regulatory fine is imposed on the Processor resulting from the Controller's instructions, the Controller's breach of this Agreement, or the Controller's violation of Applicable Data Protection Laws, the Controller shall reimburse such fine under the same terms, mutatis mutandis.

19.5 Insurance

The Processor shall maintain insurance coverage commercially appropriate to the nature, scope, and scale of its business and the Services, which may include: (a) commercial general liability insurance; (b) professional liability / errors and omissions insurance; (c) cyber liability and privacy insurance covering data breaches, privacy violations, network security failures, and notification costs; and (d) workers' compensation insurance as required by law. The Processor shall use commercially reasonable efforts to maintain coverage amounts commensurate with industry standards for similarly situated SaaS providers. Upon the Controller's written request, the Processor shall provide a summary of its current insurance coverage (subject to redaction of

commercially sensitive terms). The Processor shall notify the Controller within thirty (30) calendar days of any material reduction in, or cancellation of, its cyber liability coverage.

19.6 Injunctive Relief

Each Party acknowledges that a breach of Sections 3.4 (Prohibited Processing), 21 (Confidentiality), or any unauthorized Processing may cause irreparable harm for which monetary damages alone are insufficient. Each Party is entitled to seek injunctive or other equitable relief in any court of competent jurisdiction, without the necessity of posting a bond, in addition to all other remedies.

19.7 Limitation Period

Claims under this Agreement must be brought within two (2) years of the date the claiming Party became aware (or should reasonably have become aware) of the claim, except that claims for indemnification may be brought within three (3) years, and claims related to regulatory fines may be brought within the applicable statute of limitations.

19.8 Disclaimer of Warranties

EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, THE PROCESSOR PROVIDES THE SERVICES AND ITS DATA PROCESSING CAPABILITIES ON AN “AS IS” AND “AS AVAILABLE” BASIS WITH RESPECT TO DATA PROTECTION FEATURES. THE PROCESSOR DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE. THE PROCESSOR DOES NOT WARRANT THAT THE SECURITY MEASURES WILL BE UNBREACHABLE OR THAT THE SERVICES WILL BE ERROR-FREE, UNINTERRUPTED, OR FREE OF VULNERABILITIES. THIS DISCLAIMER DOES NOT LIMIT THE PROCESSOR’S EXPRESS OBLIGATIONS UNDER THIS AGREEMENT, INCLUDING ITS OBLIGATIONS TO IMPLEMENT AND MAINTAIN TOMS (SECTION 7), NOTIFY BREACHES (SECTION 8), AND COMPLY WITH APPLICABLE DATA PROTECTION LAWS.

20. TERM AND TERMINATION

20.1 Term. This Agreement is effective from the Effective Date and continues for the duration of the Principal Agreement and any period during which the Processor continues to Process Personal Data.

20.2 Termination for Breach. Either Party may terminate upon material breach uncured within thirty (30) calendar days of written notice.

20.3 Immediate Termination/Suspension. The Controller may suspend data transfers and/or terminate immediately if: (a) a Supervisory Authority orders suspension; (b) material breach of SCCs or transfer mechanisms; (c) failure to comply with binding court or regulatory decisions; (d) ongoing material risk from a Personal Data Breach; (e) Processor notifies inability to meet

CCPA/CPRA obligations; (f) insolvency, liquidation, receivership, or administration; (g) Processor materially breaches Section 3.4 (Prohibited Processing); or (h) Processor's government access warranty (Section 11.3) ceases to be true.

20.4 Effects. Upon termination: (a) immediate cessation of Processing (except orderly wind-down); (b) compliance with Section 13; and (c) transition assistance per Section 13.4.

20.5 Survival. Sections 1.3, 3.3, 3.4, 8, 11, 12, 13, 16, 17.2, 19, 21, 22, and all applicable Schedules survive termination.

21. CONFIDENTIALITY

21.1 Each Party shall treat this Agreement's terms and all Personal Data as Confidential Information. The receiving Party shall: (a) not disclose to third parties without prior written consent, except to Authorized Persons and professional advisors bound by equivalent obligations, or as required by law; (b) use only for this Agreement's purposes; and (c) apply at least the same care as for its own confidential information of like nature, but no less than reasonable care.

21.2 Survival. Confidentiality obligations survive for five (5) years after termination, or for as long as trade secret protection applies, whichever is longer.

21.3 Exclusions. Standard confidentiality exclusions apply (public knowledge, independent development, rightful receipt from third parties, prior possession without obligation).

22. GENERAL PROVISIONS

22.1 Governing Law. This Agreement is governed by the laws of the State of Illinois, without regard to conflict-of-law principles. This choice shall not limit Data Subject rights under mandatory provisions of Applicable Data Protection Laws.

22.2 Dispute Resolution. Disputes shall be resolved as follows: (a) the Parties shall first attempt good-faith negotiation for thirty (30) days; (b) if unresolved, disputes shall be submitted to binding arbitration administered by the American Arbitration Association (AAA) under its Commercial Arbitration Rules, before a single arbitrator, in Chicago, Illinois; (c) the arbitrator may award injunctive relief; (d) judgment on the award may be entered in any court of competent jurisdiction. Notwithstanding the foregoing, either Party may seek injunctive relief in any court per Section 19.7. Data Subject claims are not subject to mandatory arbitration.

22.3 Entire Agreement. This Agreement (including Schedules and Annexes) and the Principal Agreement constitute the entire agreement regarding Processing of Personal Data, superseding all prior communications.

22.4 Amendments. Amendments require written agreement signed by both Parties, except: the Processor may update this DPA to reflect changes in Applicable Data Protection Laws or regulatory guidance, provided that: (a) updates do not materially reduce Controller rights or data protections; (b) thirty (30) calendar days' prior notice; (c) the Controller may object within the notice period; (d) if objection is not resolved within thirty (30) days, the Controller may terminate the affected Services with a pro-rata refund.

22.5 Severability. Invalid provisions shall be reformed to the minimum extent necessary to preserve original intent. Remaining provisions continue in full force.

22.6 No Waiver. Written waiver required. Failure to enforce is not a waiver.

22.7 Assignment. No assignment without prior written consent, except: (a) to an affiliate assuming all obligations (with notice to the other Party); or (b) in connection with a merger, acquisition, or asset sale (with notice and assumption of obligations). Prohibited assignments are void.

22.8 Notices. Written notices by hand delivery, overnight courier, registered mail, or email (with confirmed receipt). Sent to addresses in the Principal Agreement or as updated in writing.

22.9 Force Majeure. Obligations excused for circumstances beyond reasonable control, except: data security (Section 7), breach notification (Section 8), confidentiality (Section 21), data deletion (Section 13), and government access (Section 11) obligations are NOT excused.

22.10 Third-Party Beneficiaries. Data Subjects are intended third-party beneficiaries to the extent required by Applicable Data Protection Laws and the SCCs. No other third-party beneficiaries except as stated.

22.11 Counterparts and Electronic Execution. Counterparts permitted. Electronic signatures (DocuSign, Adobe Sign, or equivalent) are valid originals.

22.12 SCCs Integration. Where applicable, the SCCs (Annex A) are integral. SCCs prevail over this DPA in conflict. The Schedules serve as SCC Annexes where applicable.

22.13 Version Control. This DPA is published at https://dealmatrixcrm.com/legal/dpa with version control. The Processor shall maintain an archive of prior versions, available on request. The applicable version is that in effect at the Effective Date, subject to amendments per Section 22.4.

22.14 Export Controls and Sanctions. The Processor shall comply with all applicable export control laws and economic sanctions regulations (including U.S. EAR, ITAR, and OFAC; EU sanctions regulations; and UK sanctions). The Processor shall not export, re-export, or transfer Personal Data to any sanctioned country, entity, or individual. The Processor represents that it is not on any restricted party list.

22.15 Anti-Corruption. Each Party shall comply with all applicable anti-corruption and anti-bribery laws, including the U.S. Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010.

22.16 Publicity. Neither Party shall use the other Party’s name, trademarks, or logos in any publicity, advertising, or marketing materials without the other Party’s prior written consent, except as required to perform obligations under this Agreement.

SCHEDULE 1: DETAILS OF PROCESSING (SCC ANNEX I)

Complete prior to execution. Serves as SCC Annex I where applicable.

Item	Description
A. Data Exporter (Controller)	As specified in the applicable Order Form or Principal Agreement.
B. Data Importer (Processor)	Phoenix Holdings LLC, [Address — To Be Inserted], privacy@dealmatrixcrm.com
C. Subject Matter	Processing of Personal Data to provide Deal Matrix CRM, a customer relationship management platform as set forth in the Principal Agreement.
D. Nature of Processing	Collection, storage, organization, structuring, retrieval, use, hosting, display, transmission, backup, indexing, search, analytics, and erasure of Personal Data as necessary to deliver the Services, including [e.g., account management, authentication, authorization, customer support, billing, notifications, reporting, integration].
E. Purpose of Processing	To provide, maintain, support, secure, and improve the Services; fulfill Controller instructions; comply with applicable legal obligations. Specific purposes: account and user management; CRM data storage and retrieval; deal and pipeline management; contact and company management; calendar synchronization; document and file storage; transactional email notifications; AI-assisted data import and field mapping; analytics and reporting; billing and subscription management (when activated); customer support.
F. Duration	Term of Principal Agreement plus applicable transition and retention periods (Section 13).
G. Data Subject Categories	Customer's employees, contractors, authorized end users, business contacts, prospective clients, deal counterparties, website visitors, and support requestors
H. Personal Data Types	Contact names, email addresses, telephone numbers, postal addresses, job titles, company/organization names and details, deal/opportunity data (values, stages, pipeline status, notes, activity history), calendar events and meeting data, file uploads (documents, logos, valuation reports), user account data (name, email, profile photo, role, organization membership), IP addresses, device identifiers, browser type and version, usage and behavioral data (feature usage, click patterns, session duration), account credentials (hashed and salted), payment and billing data (tokenized, when Stripe is activated), communication records (email templates, notes, activity logs), geolocation data (IP-derived), cookie identifiers, timezone, language preferences, OAuth tokens (encrypted, for Google Calendar sync)
I. Sensitive / Special Category Data	None anticipated. The Services are not designed to process special category data. If sensitive data is uploaded by the Controller in the

	course of using the Services, the Controller is solely responsible for ensuring a lawful basis and must notify the Processor in advance.
J. Transfer Frequency	Continuous real-time during active use of the Services; periodic batch processing for analytics, reporting, and backup purposes; on-demand via API integrations (e.g., Google Calendar sync, AI field mapping).
K. Retention Period	Per Section 13. For the duration of the Principal Agreement, plus the ninety (90) day transition period, plus thirty (30) days for secure deletion. Backup rotation: up to one hundred eighty (180) calendar days.
L. Competent Supervisory Authority	Illinois Attorney General; California Privacy Protection Agency (CPPA); and/or the applicable Supervisory Authority based on Data Subject location.
M. Data Storage Locations	United States (Vercel/AWS us-east-1, Supabase us-east-1). Cloudflare Edge Network (global CDN with points of presence worldwide). Additional regions available upon request.
N. Data Exporter DPO Contact	As designated by the Customer in its account settings or Order Form.
O. Data Importer DPO Contact	As designated by the Customer in its account settings or Order Form.

SCHEDULE 2: TECHNICAL AND ORGANIZATIONAL MEASURES (SCC ANNEX II)

Subject to continuous improvement; updates shall not materially decrease protection.

Domain	Measures
Access Control	RBAC; least-privilege; MFA (all admin/privileged); SSO (SAML 2.0/OIDC); SCIM provisioning/de-provisioning; PAM; quarterly access certifications; session management (timeout, concurrent limits); IP allowlisting; just-in-time access for production.
Encryption	AES-256 at rest; TLS 1.2+ in transit (1.3 preferred); HSTS; HSM-backed key management with automated rotation; encrypted DB connections; FDE on endpoints; encrypted backups (segregated keys); CMEK/BYOK option (tier-dependent).
Network Security	Defense-in-depth; segmentation/micro-segmentation; NGFW with DPI; IDS/IPS; DDoS mitigation; WAF; DNSSEC; zero-trust admin access; egress filtering; data exfiltration detection; network anomaly detection.
Application Security	Secure SDLC; OWASP Top 10 / SANS 25; SAST, DAST, SCA in CI/CD; peer code review; dependency scanning; input validation/output encoding; CSP/security headers; API rate limiting/auth; container/image scanning; SBOM generation.
Monitoring & Logging	24/7 SOC; SIEM with correlation/anomaly detection; centralized logging (12mo min, 24mo security); DAM; FIM; UEBA; CSPM; real-time alerting with escalation; tamper-evident log storage.
Vulnerability Mgmt	Continuous scanning; annual pen test (black/gray box + app layer); bug bounty; patch SLAs (critical:24h, high:7d, med:30d, low:90d); CIS Benchmarks; configuration drift detection.
Physical Security	Tier III+ DCs; SOC 2 II / ISO 27001 certified; multi-factor physical access; 24/7 security + CCTV (90d); mantrap; environmental controls; visitor mgmt with escort; media destruction.
BCP/DR	Board-approved BCP/DR; annual testing; geo-distributed redundancy; defined RTO/RPO per tier; automated failover; backup integrity testing; pandemic/supply-chain contingency; cross-region replication.
Personnel	Background checks; onboarding + annual security training with phishing sims; privileged-user training; AUP, clean desk, screen lock; NDAs; disciplinary procedures; immediate revocation on exit; exit interviews.
Data Management	Classification (public/internal/confidential/restricted); pseudonymization/tokenization; minimization by design/default; DLP (endpoint/network/cloud); NIST 800-88 deletion; data inventory/mapping; privacy-by-design; non-prod masking.
Incident Response	NIST 800-61 aligned; 24/7 on-call IR team; semi-annual tabletop exercises; external forensics retainer; automated containment; post-incident review/RCA; pre-drafted comms templates; IR metrics/KPIs.

Third-Party/Supply Chain	Risk-tiered vendor assessment (SIG/CAIQ); contractual security/privacy; annual critical vendor reassessment; right-to-audit; supply chain integrity; fourth-party monitoring; SBOM for critical deps.

SCHEDULE 3: APPROVED SUB-PROCESSORS (SCC ANNEX III)

Current list at https://dealmatrixcrm.com/legal/sub-processors. Updates per Section 6. Subscribe at https://dealmatrixcrm.com/legal/sub-processors#subscribe.

Sub-processor	Legal Entity	Location	Transfer Mech.	Processing Activities
Vercel	Vercel, Inc.	USA	N/A (domestic)	Application hosting, deployment, serverless compute, Edge CDN
Supabase	Supabase, Inc.	USA	N/A (domestic)	PostgreSQL database hosting, file/object storage (vault documents, logos, valuations)
Clerk	Clerk, Inc.	USA	N/A (domestic)	User authentication, session management, organization/tenant management
Resend	Resend, Inc.	USA	N/A (domestic)	Transactional email delivery (notifications, invitations, alerts)
Google Calendar	Google LLC	USA	N/A (domestic)	Two-way calendar synchronization via OAuth (Google Calendar API)
Sentry	Functional Software, Inc.	USA	N/A (domestic)	Application error monitoring, performance tracking, crash reporting
Anthropic	Anthropic, PBC	USA	N/A (domestic)	AI-powered features (import field mapping, data classification)
Cloudflare	Cloudflare, Inc.	USA (global edge)	N/A (domestic); SCCs for EU edge nodes	DNS management, CDN, DDoS protection, SSL/TLS termination
Stripe *	Stripe, Inc.	USA / Ireland	N/A (domestic); DPF / SCCs for EU	Payment processing, billing, subscription management (pending activation)
Upstash *	Upstash, Inc.	USA	N/A (domestic)	Redis-backed rate limiting and request throttling (pending activation)
Mailchimp *	The Rocket Science Group LLC (Intuit)	USA	N/A (domestic)	Email marketing campaigns and subscriber management (pending activation)

SCHEDULE 4: CROSS-BORDER TRANSFER MECHANISMS

Supplements SCC Annex I, Section C. Updated as mechanisms change.

Mechanism	Configuration
EU SCCs (2021/914)	Module 2 (C2P) and/or Module 3 (P2P). Clause 7 (Docking): included. Clause 9: Option 2 (general auth, 30-day objection). Clause 11: optional redress included. Clause 13(a): SA of Controller's EU establishment. Clause 17 Option 1: law of Controller's EU establishment (Ireland if none). Clause 18(b): courts of same. Supplemented by TIAs. Full SCCs as Annex A.
UK IDTA / Addendum	UK Addendum to EU SCCs or standalone IDTA under DPA 2018 §119A, with Part 2 mandatory clauses. SA: UK ICO.
Swiss FADP	EU SCCs as recognized by Swiss FDPIC, with required amendments (GDPR refs include FADP; EU/EEA refs include Switzerland; legal entities covered per revised FADP).
EU-U.S. DPF	Where data importer is DPF self-certified (EU-U.S., UK Extension, Swiss-U.S.). Processor monitors certification; 5 business day notice if certification lapses or is revoked.
Adequacy Decisions	Where European Commission, UK SoS, or Swiss FDPIC has issued adequacy. Processor monitors validity; 5 business day notice if revoked/suspended/challenged.
Supplementary Measures	Per TIA: (a) technical: additional encryption, in-use encryption, pseudonymization, key mgmt outside destination, split processing; (b) organizational: strict access policies, transparency reporting, compliance audits; (c) contractual: commitment to challenge govt requests using all legal remedies, notify Controller, minimize disclosure. Documented in TIA records.

SCHEDULE 5: JURISDICTION-SPECIFIC ADDENDA

The following apply where Personal Data is subject to the identified jurisdiction's laws.

Jurisdiction	Supplementary Terms
EU/EEA (GDPR)	Processor per Art. 4(8). Arts. 28–36 apply in full. Chapter III Data Subject rights. SA per Schedule 1.
UK (UK GDPR)	GDPR refs read as UK GDPR (DPA 2018). SA: UK ICO. UK IDTA/Addendum for Restricted Transfers.
Switzerland (FADP)	GDPR includes FADP. SA: Swiss FDPIC. EU/EEA includes Switzerland. Legal entities covered per revised FADP.
California (CCPA/CPRA)	Service Provider per §1798.140(ag). See Section 14.1. SA: CPPA and California AG.
Virginia (VCDPA)	Processor per Va. Code §59.1-575. Consumer rights: access, correction, deletion, portability, opt-out (targeted advertising, sale, profiling). DPA per §59.1-580.
Colorado (CPA)	Processor per C.R.S. §6-1-1303(17). DPA per §6-1-1309. SA: Colorado AG.
Connecticut (CTDPA)	Processor per Conn. Gen. Stat. §42-515(24). DPA per §42-520.
Utah (UCPA)	Processor per Utah Code §13-61-101. Consumer rights: access, deletion, portability, opt-out (sale, targeted advertising). SA: Utah AG.
Texas (TDPSA)	Processor per Tex. Bus. & Com. Code §541.001(24). DPA per §541.107. SA: Texas AG.
Oregon (OCPA)	Processor per ORS §646A.570. DPA per §646A.578.
Montana (MCDPA)	Processor per Mont. Code §30-15-301. SA: Montana AG.
Iowa (ICDPA)	Processor per Iowa Code §715D.1. SA: Iowa AG.
Indiana (INCDPA)	Processor per Ind. Code §24-15-1. SA: Indiana AG.
Tennessee (TIPA)	Processor per Tenn. Code §47-18-3601. SA: Tennessee AG.
Delaware (DPDPA)	Processor per Del. Code title 6 §12D-101. SA: Delaware DOJ.
New Hampshire (NHPA)	Processor per N.H. Rev. Stat. §507-H:1. SA: New Hampshire AG.
New Jersey (NJDPA)	Processor per N.J. Stat. §56:8-166. SA: New Jersey AG.
Nebraska (NDPA)	Processor per Neb. Rev. Stat. §87-1101. SA: Nebraska AG.
Maryland (MODPA)	Processor under MODPA. Sensitive data sale prohibited. Targeted advertising restrictions. SA: Maryland AG.

Minnesota (MCDPA-MN)	Processor under Minn. Stat. §325O. SA: Minnesota AG.
Kentucky (KCDPA)	Processor per Ky. Rev. Stat. §367.401. SA: Kentucky AG.
Rhode Island (RIDTPPA)	Processor per R.I. Gen. Laws §6-48.1-1. SA: Rhode Island AG.
Brazil (LGPD)	Operator per Art. 5(VII). SA: ANPD. Chapter III Data Subject rights.
Canada (PIPEDA)	Processor per PIPEDA Principles. SA: OPC. Provincial laws (Alberta PIPA, BC PIPA, Quebec Law 25) apply where applicable.

SCHEDULE 6: HIPAA BUSINESS ASSOCIATE AGREEMENT (BAA) REFERENCE

This DPA does not constitute a HIPAA Business Associate Agreement. If the Controller is a Covered Entity or Business Associate under HIPAA (45 CFR Parts 160 and 164) and will transmit Protected Health Information (PHI) to the Processor, a separate BAA must be executed prior to any Processing of PHI.

The Processor offers a standard BAA for eligible service tiers. To request a BAA, contact: legal@dealmatrixcrm.com.

Until a BAA is duly executed by both Parties: (a) the Controller shall not submit PHI to the Services; (b) the Processor has no obligations under HIPAA with respect to data received via the Services; and (c) the Processor may delete any PHI inadvertently received and notify the Controller.

Where a BAA is executed, it shall supplement (and not replace) this DPA. In the event of conflict between the BAA and this DPA regarding PHI, the BAA shall prevail.

SCHEDULE 7: U.S. STATE BREACH NOTIFICATION REFERENCE

This Schedule summarizes applicable U.S. state breach notification requirements. The Processor shall assist the Controller in meeting these timelines per Section 8.6. This is a reference guide; the Controller should consult legal counsel for jurisdiction-specific compliance.

State	Notification Timeline	AG Notification	Key Notes
California	Expedient, without unreasonable delay	AG if >500 residents	Health data: 15 business days. Consumer report required.
New York	Expedient, without unreasonable delay	AG, DFS, DOS	SHIELD Act: broadened definitions.
Texas	60 days	AG if >250 residents	Written notice or electronic.
Florida	30 days	AG within 30 days if >500	FIPA: individual notice within 30 days.
Illinois	As expedient as possible, without unreasonable delay	AG if >500 residents	BIPA applies for biometric data.
Massachusetts	As soon as practicable	AG and OCABR immediately	201 CMR 17.00 security requirements.
Virginia	60 days	AG within 60 days	VCDPA also applies to consumer data.
Colorado	30 days	AG within 30 days	CPA also applies to consumer data.
Connecticut	60 days	AG within 60 days	CTDPA also applies.
Washington	30 days	AG within 30 days if >500	Health data: specific requirements.
Oregon	45 days	AG within 45 days if >250	OCPA also applies.
Maryland	45 days	AG within 45 days	MODPA also applies.
All Other States	Varies (30–90 days)	Varies by state	Processor to maintain current 50-state matrix.

The Processor shall maintain a current 50-state (plus DC, territories, and federal) breach notification compliance matrix and make it available to the Controller upon request.

EXECUTION

This DPA may be accepted by: (a) physical or electronic signature below; (b) electronic acceptance (click-through, check-box, or digital signature) during account registration, subscription, or order; or (c) continued use of the Services after publication at the Processor's designated URL. Acceptance by any method constitutes a binding agreement.

DATA CONTROLLER (CUSTOMER)	DATA PROCESSOR (PROVIDER)
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Entity: _____	Entity: _____
Date: _____	Date: _____

——— END OF DATA PROCESSING AGREEMENT ———