ready COMPUTING

Solutions, Consultation, Implementation, and Managed Services

CORP POL-0008
Corporate Privacy Policy

August 2026

Version 13.0

READY COMPUTING

325 Hudson Street, Floor 4
New York, NY 10013-1004

Moulsham Mill, Parkway
Chelmsford, Essex, CM2 7PX (EMEA)

CERTIFICATIONS

HITRUST CSF Certified

DPF DATA PRIVACY FRAMEWORK PROGRAM

TABLE OF CONTENTS

1 INTRODUCTION

Ready Computing ("Company"), is a corporate group of entities defined below, that prioritizes the rights and privacy of its Data Subjects. As a Company that conducts business worldwide, it observes and follows all applicable frameworks, privacy laws, regulations, and requirements regarding data privacy. For a more comprehensive overview of the security controls in place that help protect privacy and data, please make a formal request to the Company contact listed below.

1.1 Purpose

Ready Computing (the "Company") is committed to establishing, implementing, maintaining, and continually improving its global privacy protections to safeguard the fundamental rights and freedoms of all Data Subjects whose personal data is processed under our responsibility. The primary purpose of this Corporate Privacy Policy is to serve as our official, public-facing Privacy Notice. It transparently codifies:

1. The specific categories of personal data, electronic Protected Health Information (ePHI), and Controlled Unclassified Information (CUI) we collect, process, and store.
2. The specific business, operational, and technical purposes for which this information is collected and processed.
3. The third-party processors, subcontractors, and legal jurisdictions to which this data may be transferred.
4. The technical, physical, and organizational measures (TOMs) we actively enforce to protect data integrity and confidentiality.
5. The statutory and contractual mechanisms enabling Data Subjects to exercise their rights of access, rectification, objection, portability, and erasure.

This policy is designed to satisfy the strict public disclosure and transparency mandates of the General Data Protection Regulation (GDPR) Articles 13 and 14, the HIPAA Privacy Rule, the EU-U.S. Data Privacy Framework (DPF), and all U.S. State Privacy laws.

1.2 Scope

This policy applies universally to all personal data processing activities executed by, or on behalf of, Ready Computing and its active wholly-owned global subsidiaries:

- **Ready Ventures LLC** (U.S. Parent Holding Company)
    - **Ready Computing LLC** (U.S. Operational Entity)
    - **Ready Computing Commercial Solutions LLC** (U.S. Commercial Entity)
    - **Ready Computing Government Solutions LLC** (U.S. Federal/State Entity)
    - **Ready Computing Innovations LLC** (U.S. Intellectual Property Entity)
- **Ready Computing Limited** (UK and EMEA Operations – Chelmsford, England)

1.2.1 Planned German Market Entry and Entity Establishment Strategy

As of the current revision of this policy, Ready Computing has not formally entered the German market. The incorporation of **Ready Computing GmbH** (Munich, Germany) is actively planned for late 2026 or early 2027.

In strict compliance with **ISO 9001:2015 Clause 6.3** and **ISO/IEC 27001:2022 Clause 6.3 (Planning of Changes)**, this upcoming expansion is managed as a controlled organizational change. Our defined market entry strategy is actively executed, resourced, and tracked via **Master Risk and Opportunity Register.**

No personal data of German data subjects is currently processed under the independent controller responsibility of a German subsidiary. Prior to the formal launch of German operations, this policy, our master Record of Processing Activities (**QMS REC-0027**), and our central compliance matrices will be updated and approved by the Data Protection Officer (DPO) to transition the German entity from "transitional" to "active" status.

All active global administrative and communication workflows are remote-first, utilizing logically segregated U.S.-hosted cloud infrastructure. All physical mailing, legal notices, and corporate asset transfers are centralized at our New York correspondence node:

- **Ready Computing 325 Hudson Street, Floor 4 New York, NY 10013**

1.2.2 Data Lifecycles and Processing Roles

This policy covers the following processing categories:

1. **Ready Computing as a Data Controller:** We act as the Data Controller for personal data relating to our global workforce (W-2 employees, 1099 independent contractors, job applicants), corporate B2B client contacts, prospective leads, and public website visitors.
2. **Ready Computing as a Data Processor:** For our core Service Delivery Management (SDM) lines—specifically **Managed Hosting** and **Client Data Integration**—we act strictly as a **Data Processor** or **HIPAA Business Associate**. In these scenarios, the Client remains the sole Data Controller. We process, translate, and host patient clinical feeds (ePHI, SDoH, and pediatric records) solely upon the documented instructions of the Client, as legally bounded by executed **Business Associate Agreements (BAAs)** and **Data Processing Addenda (DPAs)**.

1.2.3 Compliance Statement, References, and Sources

Ready Computing, and all affiliated entities declare compliance with the following:

- The EU and UK General Data Protection Regulation (GDPR)
- The Data Privacy Framework Program (DPF)
    - EU-U.S. Data Privacy Framework (EU-U.S. DPF)
    - UK Extension to the EU-U.S. DPF

      Note: Please refer to Appendix D: Compliance with the DPF and its Principles for additional information.
- United States Data Privacy Laws (i.e., All states)
    - Please refer to Appendix B: References and Sources for references and sources.
- United States HIPAA

1.2.4 Exclusions

This policy does not apply to:

- Processing activities executed within entirely client-owned, client-managed, and client-configured environments where Ready Computing personnel have no logical access, administrative oversight, or data custody.
- Non-material administrative process adjustments that do not collect, transfer, or alter the risk posture of personal data.

1.3 Audience

This policy is publicly accessible and is intended for:

- **Website Visitors and Public Users:** Individuals accessing readycomputing.com or any associated corporate web portals.
- **Clients and Integration Partners:** Current and prospective B2B clients, technology alliance partners, and authorized subcontractors.
- **Global Workforce Members:** All full-time and part-time W-2 employees, 1099 independent contractors, and job applicants.
- **Regulatory Bodies and Auditors:** External assessors evaluating our compliance under **ISO 9001:2015**, **ISO/IEC 20000-1:2018**, **ISO/IEC 27001:2022**, **CMMC Level 2**, and **HITRUST CSF**.

All Ready Computing workforce members are required to read, understand, and adhere to the security and privacy principles derived from this policy, as operationalized within the **CIPS Handbook**.

1.4 General Information

To ensure independent, board-level oversight and strict adherence to global privacy laws, the Executive Leadership Team (ELT) has formally appointed a central **Data Protection Officer (DPO)**. Pursuant to **GDPR Articles 37, 38, and 39** and **Company Policy**, this role is held by:

- **VP of Compliance and Risk Management (DPO)**
    - **Ready Computing 325 Hudson Street, Floor 4, New York, NY 10013**
    - **Contact Email:** quality@readycomputing.com

The DPO operates with complete organizational independence from daily financial (GAAP) and sales operations, holding direct reporting lines to the Founder and CEO. The DPO is the final authority for approving all Data Protection Impact Assessments (DPIAs), Legitimate Interest Balancing Tests (LIBTs), and data mapping registries.

1.4.1 Privacy Inquiries and Data Subject Requests (DSRs)

Data Subjects may submit formal inquiries, register complaints, or exercise their statutory privacy rights (including the right to access, correct, delete, restrict processing, object, or request data portability). All requests are systematically triaged, logged, and fulfilled within statutory timelines (30 calendar days for GDPR; 45 calendar days for CCPA/State laws) per **published procedure**.

- **Electronic Intake Portal:** privacy@readycomputing.com
- **Mailing Address:** Attn: DPO, Ready Computing, 325 Hudson Street, Floor 4, New York, NY 10013

Inquiries, Complaints, and External Contacts

The following links are external to Ready Computing and may be used by Data Subjects and interested parties to contact relevant authorities, file complaints, or research additional information, at any time:

- European Data Protection Supervisor (EU)
- Information Commissioner's Office (UK)
- U.S. Department of Commerce's Data Privacy Framework Program (DPF)
- United States Council for International Business
- U.S. Department of Health and Human Services (HHS)

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, Ready Computing commits to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO), and the Gibraltar Regulatory Authority (GRA) regarding unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF.

1.4.2 Investigative and Enforcement Powers of the FTC

The Federal Trade Commission has jurisdiction over Ready Computing's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF.

1.4.3 Investigative and Enforcement Powers of the U.S. Department of HHS

The U.S. Department of HHS has jurisdiction over Ready Computing's compliance with HIPAA.

1.5 Training and Awareness

A knowledgeable and vigilant workforce is our primary line of defense in maintaining a secure, compliant operational environment.

1. **Mandatory Onboarding Training:** In accordance with the **(Compliance Training and Awareness Oversight Policy)** and **HR Procedure**, all incoming personnel are required to read, complete, and formally sign an acknowledgment of the **CIPS Handbook** during onboarding.
2. **LMS Integration and Competency Mapping:** Formal privacy and security training—including specialized **HIPAA/HITECH 2026** and **GDPR/ePrivacy** modules—is delivered and tracked via our centralized **Schoox Learning Management System (LMS - CI-0010)**.
3. **Phishing Simulations:** Managed Services and IT Security conduct recurring simulated social engineering and phishing campaigns via **KnowBe4**.
4. **Annual Refreshers:** All personnel must complete an annual privacy and security awareness retraining cycle. All completion metrics and test scores are logged in the **Schoox Compliance Training Records** to satisfy **ISO 9001 Clause 7.2 (Competence)**.

1.6 Confidentiality Statement

The public-facing version of this Corporate Privacy Policy is published openly on our corporate website. However, all internal governance artifacts, security architecture manuals, system security plans (SSPs), raw

data mapping files, and filled ROPA spreadsheets referenced herein are classified as **Highly Confidential - Internal Use Only**.

Any unauthorized review, retransmission, dissemination, or copying of our internal security configurations, system boundaries, or log telemetry without the expressed, documented consent of the VP of Compliance and Risk Management is strictly prohibited and will result in immediate progressive disciplinary action up to termination of employment or contract, and potential legal prosecution. Unintended recipients must immediately contact the Company at quality@readycomputing.com and destroy all copies.

2 CORPORATE PRIVACY PROGRAM OVERVIEW

Ready Computing systematically operationalizes the protection of personal data, electronic Protected Health Information (**ePHI**), and Controlled Unclassified Information (**CUI**) by embedding the **seven (7) core data protection principles** of the **General Data Protection Regulation (GDPR) Article 5** directly into our global technical architecture and administrative workflows. These principles govern every phase of our data lifecycles across all corporate and subsidiary environments.

2.1 Lawfulness, Fairness, and Transparency

- **Operational Execution:** All processing of personal data is mapped to a specific, validated lawful basis under **GDPR Article 6** (and **Article 9** for Special Category Data). Legitimate Interest is relied upon only when supported by a formal, DPO-approved **Legitimate Interest Balancing Test (LIBT)**.
- **State-Level Consent Alignment:** To satisfy the strict requirements of the **California Consumer Privacy Act (CCPA/CPRA)**, the **New Jersey Privacy Protection Act (NJPPA)**, the **Washington My Health My Data Act (MHMDA)**, and the **Nevada Consumer Health Data Privacy Law (CHDPL)**, we enforce an **affirmative, opt-in consent model** for all sensitive data processing.
- **NJ Financial Data Perimeter:** In strict compliance with the **NJPPA**, any collection or processing of a New Jersey resident's **financial information** (including bank routing details, credit card numbers, or online portal log-in credentials) requires **explicit, affirmative opt-in consent** prior to ingestion.
- **Cookiebot CMP Integration:** Public web tracking is blocked at the perimeter. No non-essential analytical or marketing cookies (such as **Google Analytics** or **HubSpot**) execute on readycomputing.com until the visitor registers consent via our **Cookiebot Consent Management Platform (CMP)**, which logs and archives consent timestamps to ensure complete GRC transparency.

2.2 Purpose Limitation

- **Operational Execution:** Personal data is collected for specified, explicit, and legitimate purposes and is never repurposed for incompatible activities.
- **Logical Partitioning and Segregation of Duties (SoD):** To prevent unauthorized data reuse and satisfy **ISO/IEC 27001:2022 Control A.5.3 (Segregation of Duties)**, we enforce strict, logical boundaries across all SaaS and cloud systems.
    - **Finance Separation:** General billing data and accounts payable ledgers reside within an **ERP**. Access is restricted to authorized financial administrators, isolating corporate accounts from general engineering visibility.
    - **HRIS Separation:** Employee onboarding, background screening results, and performance evaluations are stored in an HRIS and are logically segregated from commercial CRM platforms.
    - **Federal/CUI Separation:** Controlled Unclassified Information is restricted to a dedicated, FIPS-compliant enclave inside Cloud Environments and is never commingled with standard commercial datasets.

2.3 Data Minimization

- **Operational Execution:** Ready Computing enforces a strict policy of collecting and processing only the **minimum personal data necessary** to achieve the stated business or contractual outcome.
- **Oregon Precise Geolocation Coarsening:** To comply with the **Oregon Consumer Privacy Act (OCPA)** ban on the unauthorized sale or sharing of precise geolocation, any device-level or network-level location tracking on our mobile or web platforms is programmatically degraded. The system automatically **coarsens location parameters** to a radius greater than **1,750 feet** (e.g., city level) prior to processing or logging in our marketing or analytics databases.
- **Testing and Development Sandboxes:** In accordance with the Company **DevSecOps Policy**, the use of live, unmasked production patient ePHI, customer PII, or federal CUI inside non-production testing, development, or training environments is **strictly prohibited**. All software testing and integration sandboxes utilize strictly synthetic or randomized dummy data.

2.4 Accuracy

- **Operational Execution:** Ready Computing takes every reasonable step to ensure personal data remains accurate, complete, and current.
- **Verification at Collection:** Data verification procedures are built into our intake webforms and portals. Administrative contact details and vendor credentials undergo formal review before setup in company Systems.
- **Self-Service Rectification:** Employees can instantly modify and correct their active profile fields (such as home address, emergency contacts, or direct deposit accounts) directly within the **BambooHR self-service portal**.
- **Correction Workflows:** External clients, prospective leads, and partners can request immediate rectification or correction of inaccurate records by submitting a verified **Data Subject Request (DSR)** to privacy@readycomputing.com, processed in accordance with Company procedure.

2.5 Storage Limitation

- **Operational Execution:** Personal data is retained only for the duration required to fulfill its designated legal, tax, or operational purpose, after which it is securely destroyed or anonymized.
- **Standardized Retention Schedules:** All retention thresholds are systematically governed by the Company's **Retention and Disposal Policy** and documented in our master **Record of Processing Activities (ROPA)**.
    - **7-Year Post-Termination Hold:** Employee personnel files, payroll histories, tax forms, client contract records, and general ledger accounts are held for exactly **seven (7) years** following separation or contract termination to satisfy IRS and statutory audit requirements.
    - **1-Year Recruitment Retention:** Candidate profiles and resume files collected during recruitment are retained for exactly **one (1) year** from the date of submission, subject to the candidate's explicit, opt-in consent. Unsuccessful applicant profiles are automatically purged annually upon expiration of the consent period.

- **Automated Platform Expiries:** In accordance with Company process and procedure, automated retention-expiry sweeps are technically configured within Company Systems to programmatically delete expired tracking cookie logs and contact metadata.
- **Annual Deletion Week:** In accordance with Company process and procedure, GRC and IT Security execute an annual coordinated deletion week to manually verify and scrub expired legacy data from Google Workspace, local workstations, and backup drives, except where suspended by a formal **Litigation Hold**.

2.6 Integrity and Confidentiality (Security)

Ready Computing enforces a comprehensive, multi-layered defensive perimeter to safeguard personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage.

- **FIPS-Validated Encryption:** In accordance with the Company's **(Encryption Configuration Policy)**, all sensitive data—including ePHI, SSNs, and federal CUI—is encrypted both at rest and in transit. Data at rest within our AWS and GCP environments is secured using **AES-256 encryption** with keys managed via FIPS 140-3 validated Hardware Security Modules (HSMs). Data in transit is secured using **TLS 1.3** forced through our network boundaries.
- **Workstation Active Defense Stack:** All corporate-issued endpoints and workstations are locked down using a unified security agent stack:
    - Enforcing a zero-trust, default-deny application allowlisting policy and strict storage ringfencing to prevent lateral data movement, unauthorized software execution, or USB mass storage copy actions.
    - Deploying advanced, next-generation EDR (Endpoint Detection and Response) and Managed Detection and Response (MDR) threat hunting to proactively neutralize malware and ransomware.
    - Automating continuous operating system checking, CVSS vulnerability scanning, and rapid patch deployment on all workforce endpoints.
    - All critical system-of-record backups—including medical datasets and employee records—are synced to segregated, cloud-native storage vaults. These backups are technically configured with write-once, read-many (WORM) immutability, mathematically preventing ransomware encryption or deletion by compromised credentials to ensure absolute disaster recovery resilience per **NIST SP 800-171 Requirement 3.8.9**.

2.7 Accountability

- **Operational Execution:** Ready Computing is legally accountable for upholding all seven (7) principles and proactively demonstrates its compliance posture to auditors, regulators, and clients.
- **The GRC SSoT Framework:** We maintain a centralized, auditable repository within our **GRC Platform** to serve as our "Single Source of Truth" (SSoT) for GRC evidence.
- **DPO Oversight:** Our **Data Protection Officer (DPO)** retains overall responsibility for maintaining and approving our risk registers, conducting GRC evaluations, and ensuring that any significant changes to our processing environments are thoroughly analyzed and signed off before deployment.

2.8 Records of Compliance (The GRC SSoT Framework)

Ready Computing formally documents and defends its global compliance posture through a structured suite of live, auditable records:

1. **Record of Processing Activities (ROPA):** Our master data inventory managed under **GDPR Article 30**. The ROPA is our authoritative registry mapping every active data flow, processing purpose, BPO delegation, data category, recipient list, and international transfer mechanism across all corporate and product divisions.
2. **Risk, Issue, Opportunity, and Continuous Improvement Register:** The central ledger where all **Data Protection Impact Assessments (DPIAs)**, security risks, system vulnerabilities, and continuous improvement opportunities are integrated and systematically scored, tracked, and mitigated using our unified **Enterprise Risk and Issue Management (ERIM) methodology**.
3. **Document Control Master List (DCML):** The authoritative register managing the lifecycle, version control, review dates, custodian delegations, and executive approvals for every policy, procedure, standard, and form within our Integrated Management System (IMS).

2.9 Audits and Program Assessments

To maintain our high-assurance certifications (**ISO 9001:2015**, **ISO/IEC 20000-1:2018**, **ISO/IEC 27001:2022**, and **HITRUST CSF r2**) and ensure continuous compliance with global regulations, our GRC program is subjected to rigorous, recurring auditing:

Internal Audits and Dual-Auditor Protocol

- **Audit Schedule:** Internal audits are executed continuously throughout the year on a formalized schedule documented in the Company **Internal Audit Schedule**.
- **The Dual-Auditor Independence Protocol:** In strict accordance with **ISO 27001 Control A.5.35** and our external audit optimization directives, Ready Computing enforces a **Dual-Auditor Protocol**. Internal audits must be conducted by at least **two (2) qualified GRC specialists** operating with complete operational independence from the specific department or process under review. This ensures that the personnel designing or managing a process (e.g., HR or IT Support) are never permitted to audit their own workflows, guaranteeing absolute audit objectivity and non-bias.

Transition to Annual Internal Privacy Audits

- **Internal Execution Strategy:** In lieu of third-party engagements, our GRC department executes a comprehensive **Annual Internal Privacy Audit every August**. These internal audits are performed using standard, validated external GRC templates and check sheets. This transition dramatically reduces administrative overhead while maintaining a highly rigorous, continuous verification loop that is fully documented in **Internal Audit Checklists** and reported directly to the CEO during quarterly reviews.

2.10 Proactive Privacy Assessments (DPIAs & LIBTs)

- **DPIA Triggers (GDPR Article 35):** We conduct a formal **Data Protection Impact Assessment (DPIA)** prior to executing any high-risk processing activity. DPIAs are mandatory for:
    1. The large-scale processing of Special Category Data (ePHI, biometrics, SDoH, or pediatric records).

2. The deployment of new, innovative, or algorithmic technologies, including generative AI models (Gemini) or AI-assisted development IDEs (Cursor) governed under Company policy.
3. The systematic, large-scale monitoring of employee endpoints or perimeters (such as active workstation logging via Company Systems).

- **LIBT Triggers (GDPR Article 6(1)(f)):** For any processing activity where Legitimate Interest is selected as the primary lawful basis, the BPO must complete a **Legitimate Interest Balancing Test (LIBT)**. No processing based on legitimate interest may commence until the LIBT is formally reviewed, passed, and signed off by the DPO.
- **Prohibition on Special Category LIBTs:** In strict accordance with **GDPR Article 9**, an LIBT alone is **legally insufficient** to justify the processing of Special Category Data (ePHI, SDoH, biometrics). Any processing of Special Category Data is strictly prohibited unless it satisfies a specific **Article 9(2) condition** and is supported by a completed, authorized **DPIA**.

3 DATA SUBJECT'S RIGHTS

Ready Computing systematically respects, upholds, and operationalizes the rights of individuals regarding the processing of their personal data, in strict accordance with the **General Data Protection Regulation (GDPR)**, the **California Consumer Privacy Act (CCPA/CPRA)**, the **HIPAA Privacy Rule**, and applicable U.S. state-level data privacy statutes (including those in Washington, Nevada, Oregon, and New Jersey).

Subject to their regional jurisdiction, Data Subjects maintain the following fundamental statutory rights, which the Company is obligated to observe:

- **The Right to Be Informed:** The right to receive clear, transparent, and easily understandable information regarding how we collect, process, share, and protect personal data, fulfilled via this public-facing policy.
- **The Right of Access:** The right to obtain confirmation from the Company as to whether their personal data is being processed, and to receive a copy of their active personal records.
- **The Right to Rectification:** The right to request the immediate correction of inaccurate or incomplete personal data held by the Company.
- **The Right to Erasure:** The right to request the deletion or removal of personal data when there is no overriding legal, tax, or contract-bound regulatory justification to continue processing.
- **The Right to Restrict Processing:** The right to "block" or suppress further processing of their personal data, during which the Company may store the data but is prohibited from active utilization.
- **The Right to Data Portability:** The right to obtain and reuse their personal data for their own purposes across different services, delivered in a structured and machine-readable format.
- **The Right to Object:** The right to object to processing based on legitimate interests or direct marketing.
- **Rights Related to Automated Decision-Making and Profiling:** The right to request human intervention, express their point of view, and contest any automated or algorithmic decisions that produce legal or similarly significant effects.

3.1 Data Subject Request (DSR) Intake and Verification Process

The Company has established a centralized, monitored, and secure intake perimeter for all privacy-related inquiries and formal requests:

- **Central Email Portal:** privacy@readycomputing.com
- **Physical Mail Node:** Attn: Data Protection Officer, Ready Computing, 325 Hudson Street, Floor 4, New York, NY 10013

In accordance with Company procedures, any workforce member who receives a communication that appears to be a formal exercise of a Data Subject's rights must forward the request to the Data Protection Officer (DPO) immediately to prevent statutory response delays.

3.1.1 Identity Verification Protocol

To prevent unauthorized data exposure, social-engineering bypasses, or malicious exfiltration, the Company enforces a rigid identity verification process prior to disclosing, altering, or deleting any personal records.

1. **Verification Methodology:** The personnel who intakes the request verifies the identity of the requesting individual utilizing proportionate, risk-based methods. This may include cross-referencing the requestor's validated email address, verifying verbal and written credentials, or confirming unique employment identifiers.
2. **Minimization of Verification Data:** In compliance with data minimization principles, the Company will not request more sensitive personal data than is strictly necessary to confirm identity.
3. **Third-Party Authorization:** If a DSR is submitted by an authorized agent (such as a legal representative or a background-screening agency), the Company requires signed, documented consent from the data subject before processing the fulfillment.

3.1.2 Processing Timelines

- **GDPR and International Requests:** Fulfillments are processed and delivered securely "without undue delay" and in all cases within **thirty (30) calendar days** of receiving a verified request.
- **U.S. State-Level Requests:** Fulfillments are completed within **forty-five (45) calendar days** of receipt, subject to statutory extensions where legally permissible.

3.2 The Processor Boundary (The Client Referral Gate)

For our core Service Delivery Management (SDM) lines of business—specifically our managed hosting, database migration, and clinical integration services—Ready Computing acts strictly as a **Data Processor** or **HIPAA Business Associate**. The B2B Client (such as a health system, health information exchange, or commercial partner) remains the sole **Data Controller** (or Covered Entity) who maintains overall legal ownership of the data.

3.2.1 Strict Referral Mandate

The personal datasets processed within our hosted environments—including patient clinical feeds, electronic Protected Health Information (ePHI), Social Determinants of Health (SDoH), and children's health records—are hosted solely upon the documented instructions of the Client, as legally bounded by executed **Data Processing Addenda (DPAs)** and **Business Associate Agreements (BAAs)**. Consequently:

- **Direct Fulfillment Prohibited:** Ready Computing is technically and contractually prohibited from directly accessing, modifying, extracting, or deleting patient clinical data in response to an individually submitted DSR.
- **Programmatic Redirection Gate:** Any direct DSR received by our support desk, engineering team, or administrative channels originating from a patient or client end-user must be immediately routed directly back to the respective B2B Client (the Data Controller).
- **Controller Authorization Required:** The Company will only execute database-level modifications, extractions, or deletions of client-owned payloads when formally directed and authorized in writing by the designated Data Controller, protecting our pipelines from unauthorized data destruction or breach of contract.

3.3 Denial and Appeal Procedures

Data Subject Rights are not absolute and may be legally restricted or exempted under specific statutory conditions. The Company may deny a DSR, in whole or in part, under the following circumstances:

- **Legal Obligations:** Where the Company is under a superseding legal obligation to retain the record (such as IRS/HMRC tax audit rules, labor law reporting, or federal contracting cost-accounting standards). For example, active or separated workforce members cannot demand the erasure of payroll, tax withholding, or direct-reimbursement vouchers.
- **Establishment, Exercise, or Defense of Legal Claims:** Where the retention of records is strictly necessary to defend the Company against potential wrongful termination, discrimination, or compliance litigation. For example, individuals who are the subject of an active or historical Fraud, Waste, and Abuse (FWA) investigation, or who have files logged in our progressive discipline registries, cannot demand the deletion of these records.
- **Technical and Provenance Integrity:** Where deletion of data would destroy essential system-engineering provenance, break repository integrity, or violate non-repudiation standards. For example, software developers cannot demand the erasure of their historical code commits, repository contributions, or system-modification audit logs, which must be permanently preserved to guarantee software supply chain security.

3.3.1 The Appeal Process

If a DSR is denied, the requesting individual has a formal right to **appeal** the decision.

- **Intake:** Appeals must be submitted to GRC at privacy@readycomputing.com within thirty (30) calendar days of receiving the denial notification.
- **Escalation Gate:** GRC logs the appeal in our centralized DSR register, linking it directly to the original DSR ID. The appeal is formally escalated to the Data Protection Officer (DPO) and senior legal counsel for an independent review.
- **Resolution:** The DPO conducts a thorough, double-check evaluation of the denial justification to minimize legal risk. A final, legally binding written determination is delivered to the individual within thirty (30) calendar days of receiving the appeal.

3.4 External Redress and Regulatory Recourse

If a Data Subject's appeal is denied, or if they remain unsatisfied with the Company's final determination, they have the right to seek external redress.

3.4.1 Data Protection Authorities (DPAs) and Attorneys General

- The Company's final appeal determination will include explicit instructions enabling the individual to escalate their complaint to the appropriate regulatory body:
- **United Kingdom:** The Information Commissioner's Office (ICO).
- **European Union:** The relevant national or state Data Protection Authority (DPA) corresponding to their region of residence.
- **United States:** The Attorney General of their state of residence (e.g., for California, New Jersey, Washington, or Nevada residents).

3.4.2 Data Privacy Framework (DPF) Recourse Mechanisms

- For complaints regarding transatlantic data transfers and compliance with the **EU-U.S. Data Privacy Framework (DPF)** and the **UK Extension**, Ready Computing has established independent recourse mechanisms to investigate individual complaints:
- **Inquiries and Disputes:** Individuals may first direct inquiries or complaints to our central DPO at privacy@readycomputing.com.
- **Independent Recourse:** If a DPF-related complaint cannot be resolved internally, individuals may submit their complaint to the independent recourse mechanism designated by the Company, details of which are provided upon request.
- **Binding Arbitration:** Under certain conditions, individuals may invoke binding arbitration for unresolved complaints.
- **Enforcement Authority:** The Federal Trade Commission (FTC) has jurisdiction over Ready Computing's compliance with the DPF Principles.

4 DATA CLASSIFICATION AND DATA SOURCING RULES

Ready Computing systematically secures and handles all information according to its value, sensitivity, and risk of unauthorized disclosure. To balance operational efficiency with robust data security, the Company enforces a centralized **three-tier information classification schema**:

1. **Public Information (PI):** Information that is intentionally disclosed, disseminated, or made available to the public. Public Information carries a negligible security risk and requires no special protections.
2. **Confidential Information (CI):** Sensitive internal business information that is restricted from public disclosure. Unauthorized exposure of Confidential Information could cause moderate financial, operational, or reputational harm to the Company, its workforce, or its commercial clients.
3. **Highly Confidential Information (HCI):** Highly sensitive, regulated, or proprietary data that requires the most stringent logical and administrative controls. Highly Confidential Information includes Protected Health Information (PHI), Personally Identifiable Information (PII) subject to regional privacy laws, financial records, federal contracting data, and core intellectual property. Unauthorized exposure of HCI would result in severe statutory, contractual, financial, and legal liabilities.

Sensitivity Tier	General Definition	Specific Corporate Examples
Public Information (PI)	Disseminated or made openly available to the public; carries minimal disclosure risk.	Finalized website copy, approved marketing brochures, public press releases, and general product catalogs.
Confidential Information (CI)	Restricted internal business data; access is limited to personnel with a business need.	Strategic corporate plans, internal policies, standard operating procedures, non-sensitive business emails, and system logs.
Highly Confidential Information (HCI)	Regulated, legally protected, or highly proprietary data; access is strictly isolated.	Patient medical records (ePHI, SDoH), employee Social Security Numbers (SSNs), bank routing details, background check results, and proprietary codebase repositories

Table 1: Data Classification Table

4.1 Automated and Manual Data Labeling

- **Systematic Metadata Tagging:** In accordance with Company policies, data classification is technically enforced across the corporate cloud ecosystem. When creating, opening, or storing files within centralized collaborative drives, the system **automatically prompts users** to select and assign the appropriate Data Sensitivity Label. These metadata tags systematically govern downstream DLP rules, restricting external sharing and download privileges based on classification severity.
- **Manual Fallback Controls:** For data formats where automated metadata tagging is not technically feasible (such as hardcopy files or specialized administrative exports), personnel are required to manually apply prominent classification labels—such as standard confidentiality statements in document footers and email headers.

4.2 Data Sourcing and Ingest Rules

Ready Computing adheres strictly to the principle of **data minimization**. We collect and process only the personal data that is directly relevant and necessary to accomplish a documented business purpose.

1. **Administrative Validation:** All corporate webforms, applicant portals, and data ingestion gateways are designed to limit collection strictly to the data fields approved and registered within the Company's master **Record of Processing Activities (ROPA)**.
2. **Prohibition of Unnecessary Sensitive Ingestion:** Intake forms are prohibited from requesting highly sensitive, unnecessary identifiers (such as SSNs or banking details) during initial, low-risk interactions, ensuring we do not accumulate toxic data liabilities.

4.2.1 Technical Ingestion Safeguards

All data entering the Company's operational perimeter is protected by strict technical gates. Inbound transmission channels enforce industry-standard **transit encryption (minimum TLS 1.2, preferring TLS 1.3)** to prevent eavesdropping and intercept attacks. Data-at-rest is ingested directly into secure, logically partitioned cloud databases where logical access is governed by federated identity providers enforcing mandatory Multi-Factor Authentication (MFA).

4.3 Candidate (Job Applicant) Processing Rules

Candidate data is sourced and ingested through controlled, compliant channels, including direct online applications, university recruitment partnerships, and vetted third-party recruitment agencies. In accordance with Company procedures, the sourcing of talent is managed to ensure equal opportunity, fair selection, and non-discriminatory hiring practices.

4.3.1 Categories of Candidate Data

During the recruitment lifecycle, the Company collects and processes the following standard categories of personal data:

- **Identity and Contact Details:** Full legal name, personal email address, physical mailing address, and mobile phone number.
- **Professional Background:** Resume details, employment history, academic qualifications, and professional certifications.
- **Interview Records:** Interview notes, performance-based assessments, and formal evaluations generated by hiring managers.

4.3.2 Equal Employment Opportunity (EEO) Data Ingestion

To comply with federal and state labor laws, the Company collects voluntary **Equal Employment Opportunity (EEO) demographic data**.

1. **Collected Categories:** This may include race, ethnicity, sex, veteran status, and disability status.
2. **Technical Segregation:** EEO data is collected via a separate, secure portal and is logically segregated from candidate resumes and screening files. Hiring managers have zero visibility into EEO selections, ensuring recruiting decisions remain entirely objective and unbiased.

4.3.3 Post-Offer Background Screening and Federal Exclusion Checks

- **Trigger and Consent:** Background checks are never performed during the initial sourcing or interviewing stages. A comprehensive background screening is triggered **strictly after a candidate has accepted a formal, written offer of employment** and provided explicit, signed consent.

- **Vetting Scope:** Post-offer screenings include criminal history verifications, academic qualification checks, and monthly checks against the **System for Award Management (SAM)** and other federal exclusion registries.
- **Ethics and Compliance Advisory Opinions:** In accordance with Company recruiting procedures, if a selected candidate is a former public or Department of Defense (DoD) official, HR must obtain and archive a written **Ethics Advisory Opinion** prior to finalizing the onboarding contract, ensuring compliance with federal revolving-door regulations.

4.4 Employee and Workforce Processing Rules

The Company's centralized **Human Resources Information System (HRIS)** serves as the secure system of record for all active and historical employee data. This database contains full legal names, SSNs, direct deposit bank routing details, physical home addresses, personal email addresses, tax withholding documentation, and emergency contact details. To ensure data accuracy, employees are provided with secure, self-service access, enabling them to instantly review, update, and correct their personal contact information, tax forms, and direct deposit selections.

4.4.1 Benefits, Retirement, and Wellness Program Administration

- **Benefits and Retirement Enrollment:** The Company processes employee personal and financial data to administer mandatory and voluntary benefits, including medical, dental, and vision insurance, and retirement (401k) accounts. Dependent and beneficiary details (such as names, dates of birth, and SSNs) are processed strictly for benefits registration and compliance with federal employee healthcare laws.
- **Wellness Programs:** Employees may optionally participate in corporate wellness and coaching initiatives. Data generated during wellness sessions is held under **joint-control frameworks** with our certified wellness vendors, ensuring individual coaching notes and health metrics are strictly insulated from general management and never influence performance appraisals or employment decisions.

4.4.2 Career Lifecycle, Performance Appraisals, and Progressive Discipline

- **Competency and Performance Appraisals:** Workforce performance metrics, bi-annual reviews, project accomplishments, and peer feedback are formally tracked in our central systems to govern merit-based raises and promotions.
- **Progressive Discipline Tracking:** If behavioral or performance issues arise, the Company enforces a structured, four-stage progressive discipline procedure (Informal Discussion, Written Warning, Performance Improvement Plan [PIP], and Termination). Disciplinary records, warning forms, and PIPs are classified as **Highly Confidential Information** and are secured within the employee's HRIS personnel file, completely restricted from standard IT support or AP view.
- **Right to Erasure Exemptions:** To prevent regulatory and legal risk, workforce members **do not possess a right to erase** their historical performance ratings, manager evaluation notes, or active progressive discipline logs. These records are permanently retained for exactly **seven (7) years** following separation to support the Company's legal defense against potential wrongful termination or labor dispute litigation.

4.4.3 Worker Legal Name Change Procedure

If an active workforce member undergoes a legal name change, the Company enforces a strict verification procedure.

1. **Documentation Validation:** The employee must submit certified legal proof of the name change (such as a marriage certificate, court order, or updated Social Security card).
2. **System-Wide Synchronization:** Upon HR approval, the change is synchronized across all core Company systems, including payroll records, tax registries, benefits databases, Google Workspace email accounts, logical system access credentials, and the central asset inventories, ensuring absolute consistency and data integrity.

4.4.4 Personnel Offboarding and System Deprovisioning

Upon receiving a formal resignation or termination notice from HR, the IT Security Department executes a closed-loop offboarding procedure.

- **Immediate Access Revocation:** Logical access to all Company cloud accounts, Google Workspace drives, code repositories, and SaaS platforms is revoked within strict SLAs (within **four hours** for high-risk departures, and by the end of the resource's final shift for standard separations).
- **Physical Asset Return:** The departing workforce member is contractually obligated to return all corporate-issued hardware assets (laptops, monitors, mobile devices).
- **Cryptographic Decommissioning:** IT Node Managers verify physical receipt of the hardware, execute a secure, NIST SP 800-88 compliant cryptographic wipe of the hard drives, and update the workstation status to "Retired" in the **Configuration Management Database (CMDB)**.

4.4.5 Contractor Misclassification Controls and Administration

To comply with IRS worker classification guidelines and mitigate financial and operational risk, the Company enforces absolute administrative separation between employees and independent contractors:

1. **Accounts Payable Processing:** All independent contractors are paid exclusively via accounts payable invoice processing in the **Company ERP System**, completely separate from our corporate employee payroll systems.
2. **Benefit Exclusions:** Contractors are strictly prohibited from enrolling in corporate benefits, 401k plans, wellness programs, or employee reward portals.
3. **Documentation Boundaries:** Contractors are blocked from accessing internal employee-only documentation, including the standard Employee Handbook. Contractor rights, security rules, and expectations are governed strictly by their executed Independent Contractor Agreement and a dedicated Contractor Handbook.

4.5 B2B Client, Partner, and Alliance Processing Rules

Ready Computing collects and processes B2B contact data to initiate, manage, and scale professional relationships with clients, integration partners, and strategic alliances. Lead data is ingested from public RFP procurement portals, inbound website inquiries, co-selling partner platforms, and corporate events.

4.5.1 Categories of B2B Contact Data

For B2B commercial entities, we collect and process:

- **Contact Information:** Name, corporate email address, business physical address, and mobile phone number.
- **Professional Details:** Job title, company name, department, and social media profile links (e.g., LinkedIn).
- **Interaction History:** Detailed notes from sales discovery calls, bid files, proposal drafts, and transaction histories.

4.5.2 Client Relationship and Satisfaction (CSAT) Monitoring

- **Automated CSAT Surveys:** To satisfy quality standards, the Company automates the collection of customer satisfaction (CSAT) and Net Promoter Scores (NPS) following the completion of billing milestones or quarterly project deliveries.
- **Escalation of Negative Feedback:** In accordance with Company procedures, any CSAT survey yielding an aggregate score **under 8.0** automatically triggers a high-priority issue in the Company's service desk. The issue is routed directly to the Chief Services Officer (CSO) and Chief Technology Officer (CTO) for a mandatory **Causal Analysis and Resolution (CAR)** investigation, ensuring process gaps are closed and documented.

4.5.3 Client-Owned Data and Clinical Payloads (The Processor Boundary)

- **The Strict Processor Boundary:** For our primary lines of business—such as managed cloud hosting, database migrations, and health integration services—Ready Computing processes, translates, and stores client-owned datasets. These datasets contain highly sensitive patient clinical feeds, electronic Protected Health Information (ePHI), Social Determinants of Health (SDoH), and pediatric records.
- **Processor Role:** In this capacity, the Company acts strictly as a **Data Processor** or **HIPAA Business Associate**. The B2B Client remains the sole **Data Controller** who holds overall legal ownership of the data.
- **No Direct DSR Fulfillment:** To prevent unauthorized data deletion and breach of contract, the Company is **prohibited from directly acting upon individually submitted patient DSRs**. Any direct patient request received by our support desks or administrators is legally and systematically redirected back to our B2B Client (the Data Controller) for authorization and fulfillment.

5 PRIVACY NOTICE BY DATA SUBJECT TYPE

In the following section of this document, the Company explicitly categorizes its Data Subjects by type to formally document the types of information we request/collect, why that information is requested/collected, what happens if the information requested is not provided, and the legal basis we rely on for the collection of that data.

5.1 Employees or Potential Employees

Ready Computing collects, processes, and stores the following categories of personal data regarding its global employment candidates, active personnel, and former workforce members:

1. **Recruitment and Identity Data:** Full legal name, personal email address, physical mailing address, mobile phone number, education history, work experience, professional certifications, and interview evaluation notes.
2. **Government and Regulatory Identifiers:** Social Security Number (SSN), National Insurance Number (or other national tax IDs), passport details, driver's license copies, and federal employment eligibility verification records.
3. **Financial and Compensation Data:** Bank account and routing numbers (for direct deposit payroll), salary rates, tax withholding elections (Forms W-4/W-4P), dependent and beneficiary names and dates of birth, loan history, and out-of-pocket business expense receipts.
4. **Special Category Demographic Data:** Voluntary, self-disclosed Equal Employment Opportunity (EEO) classifications—including race, ethnicity, sex, veteran status, and disability status—and voluntary wellness or employee coaching logs.
5. **Workstation and Security Telemetry:** Device IP addresses, hostnames, media access control (MAC) addresses, logical access logs, system modification histories, and behavioral security metrics.
6. **Directory and Interactive Mapping Data:** First name, last name, approximate corporate geolocation (i.e., City and State), and peer-to-peer social profiles in the Human Resources Management System.

5.1.1 Stated Purposes for Processing

The Company processes employee and candidate data strictly to execute the following core activities:

1. **Recruiting and Talent Selection:** Identifying, shortlisting, interviewing, and evaluating applicants for open positions.
2. **Onboarding and System Provisioning:** Performing post-offer background checks, verifying employment eligibility, setting up personnel records, and provisioning logical system access credentials.
3. **Compensation and Benefits Administration:** Processing recurring payroll, calculating tax withholdings, initiating ACH direct deposits, executing wellness programs, administering 401(k) retirement accounts, and registering medical, dental, and vision insurance benefits.
4. **Performance and Life-cycle Management:** Tracking bi-annual performance evaluations, approving merit-based raises or promotions, and managing progressive disciplinary investigations or formal warnings.

5. **Active Security and Network Defense:** Utilizing Company endpoint defense systems, monitoring network boundaries, enforcing Data Loss Prevention (DLP) rules, performing social engineering testing, and executing forensic investigations of suspected insider threats.
6. **Workforce Directory and Social Mapping:** Maintaining a secure, internal, interactive workforce directory map to display approximate locations (i.e., City and State) of personnel to facilitate team bonding, geographical awareness, and local collaboration (when necessary).

5.1.2 Lawful Basis for Processing

- **Under GDPR and UK GDPR (Article 6):**
  - **Article 6(1)(b) (Contract):** For taking pre-contractual steps at the request of an applicant, executing standard employment agreements, and processing recurring compensation.
  - **Article 6(1)(c) (Legal Obligation):** For fulfilling statutory tax reporting, labor law disclosures, and employment eligibility verifications.
  - **Article 6(1)(f) (Legitimate Interest):** For administering voluntary perks, measuring training completion rates, conducting phishing simulations, and securing corporate infrastructure.
  - **Article 6(1)(a) (Consent):** For retaining unsuccessful candidate profiles for future employment consideration.
    - Explicit, affirmative, and revocable opt-in consent is the sole legal basis relied upon for populating employee name and location pins within the internal interactive workforce map. Participation is entirely voluntary. Personnel may grant, modify, or completely withdraw their consent at any time via self-service portal settings or by submitting a request to GRC, without any negative impact on their employment status, performance appraisals, or compensation.
- **Special Category Data Conditions (Article 9):**
  - **Article 9(2)(b) (Employment Law):** For carrying out mandatory obligations in the fields of employment, social security, and social protection law, such as administering health insurance or processing tax garnishments.
  - **Article 9(2)(a) (Explicit Consent):** For processing candidate EEO demographics and employee wellness or coaching records.
  - **Article 9(2)(f) (Defense of Legal Claims):** For preserving progressive discipline records and incident logs necessary to establish, exercise, or defend against legal disputes.

5.1.3 Impact of Non-Provision

Providing personal, tax, and identity verification data is a mandatory condition of employment. If a candidate or employee objects to, or fails to provide, this required information:

- The Company will immediately terminate the recruiting, interviewing, or onboarding process.
- The Company will be unable to calculate or distribute compensation, process tax withholdings, or administer employee healthcare and retirement benefits.
- IT Security will immediately deny the provisioning of logical system credentials and retrieve any corporate-issued hardware, as the Company cannot permit unverified resources to access our secure networks.

5.1.4 Onward Transfers and Jurisdictions

All global employee data—including records for UK and European personnel—is consolidated and processed within our secure U.S. parent company's cloud-native infrastructure. To facilitate payroll and operations, the Company securely transfers employee data to:

- Authorized third-party payroll processors, benefits brokers, 401(k) administrators, and medical insurance carriers.
- Vetted background screening providers.
- State and federal tax and labor departments (e.g., IRS, HMRC, and DHS E-Verify).

These transatlantic data flows are fully protected under our active registration with the **EU-U.S. Data Privacy Framework (DPF)**, the **UK Extension**, and where applicable, standard Standard Contractual Clauses (SCCs).

5.1.5 Retention Boundaries

- **Active Personnel Files:** Retained for exactly **seven (7) years** following the formal separation or termination of employment in accordance with Company record retention policies and tax regulations.
- **Unsuccessful Candidate Profiles:** Deleted exactly **one (1) year** from the date of submission, subject to the candidate's explicit, opt-in consent.
- **Employee Support Tickets and System Change Records:** Retained indefinitely to maintain the integrity of our historical software development and system configuration change management ledgers.

5.2 Independent Contractors, Potential Contractors, and Service Contract Workers

To comply with federal worker classification standards and maintain strict administrative boundaries, the Company collects and processes the following specific categories of contractor data:

- **Business and Identity Data:** Individual or corporate business name, doing-business-as (DBA) registrations, professional job title, corporate email address, business mobile phone number, and physical mailing address.
- **Fiduciary and Transactional Data:** IRS Form W-9 details, Employer Identification Number (EIN), corporate bank account routing numbers, itemized professional invoices, and transaction histories. *In strict accordance with contractor classification boundaries, the Company does not collect or store Social Security Numbers (SSNs) for independent contractors.*
- **Background and Screening Data:** Professional and academic certifications, identity document verifications (e.g., driver's license or passport), and post-contract criminal history screening results.
- **Workstation and Security Telemetry:** Device IP addresses, hostname configurations, system access logs, and endpoint security metrics.

5.2.1 Stated Purposes for Processing

Contractor data is processed strictly for the following operational and security reasons:

1. **Contract Execution and AP Invoicing:** Drafting and executing Independent Contractor Agreements, verifying business credentials, processing professional invoices, and executing bank wire or ACH transfers.
2. **Worker Misclassification Mitigation:** Structurally segregating contractor records from general employee payroll, benefits, and wellness portals to satisfy IRS, Department of Labor (DOL), and tax auditing guidelines.
3. **Logical Access and Equipment Provisioning:** Verifying background check clear status, issuing company-owned workstations, and provisioning temporary, role-based system credentials.
4. **Workforce Security Monitoring:** Enforcing Company endpoint defense policies, analyzing system access logs, and verifying that contractors complete mandatory security awareness training before system access is granted.

5.2.2 Lawful Basis for Processing

- **Article 6(1)(b) (Contract):** For taking steps to negotiate, draft, and execute binding contractor agreements and processing professional service fees.
- **Article 6(1)(f) (Legitimate Interest):** For evaluating the operational suitability of external service providers and monitoring system access logs to secure our logical perimeters.
- **Article 6(1)(c) (Legal Obligation):** For fulfilling mandatory IRS Form 1099-NEC reporting and state tax audit requirements.
- **Article 6(1)(a) (Consent):** For executing the third-party background screening process.

5.2.3 Impact of Non-Provision

Providing business verification, tax identification, and background check data is a prerequisite to contracting. If an independent contractor objects to providing this data:

- The Company will immediately cease contract negotiations and cancel the engagement.
- The Company ERP System will block the creation of the vendor profile, preventing the processing of invoices or disbursement of service fees.
- IT Security will deny the creation of any logical credentials, preventing the contractor from accessing corporate systems or performing services.

5.2.4 Onward Transfers and Jurisdictions

Contractor business records are centralized on our U.S.-hosted cloud systems. Onward transfers are restricted to:

- The Company ERP system and contract lifecycle management platforms.
- Vetted background screening providers.
- Corporate banking partners.
- Tax authorities (e.g., IRS, HMRC).

These flows are safeguarded under our active **EU-U.S. Data Privacy Framework (DPF)** and Standard Contractual Clauses (SCCs).

5.2.5 Retention Boundaries

All executed Independent Contractor Agreements, tax filings (Forms 1099-NEC), and invoice records are held for exactly **seven (7) years** following the termination or expiration of the contractor agreement in accordance with corporate retention policies.

5.3 Vendors, Suppliers, and Potential Partners

Ready Computing collects and processes the following B2B data regarding supplier and alliance points of contact (POCs):

- **B2B Contact Details:** First and last name, business job title, company name, corporate email address, and business phone number.
- **Fiduciary and Tax Identifiers:** Federal Employer Identification Number (EIN), corporate physical address, tax withholding certifications, and bank wire/ACH routing numbers.
- **Security and Compliance Attestations:** Vendor-provided SOC 2 reports, ISO/IEC certifications, penetration testing summaries, and signed Non-Disclosure Agreements (NDAs).
- **Due Diligence and Performance Metrics:** Vendor performance scorecards, questionnaire responses, and monthly checks against federal debarment and exclusion registries.

5.3.1 Stated Purposes for Processing

Vendor and partner data is processed strictly to manage the following supply chain activities:

1. **Supply Chain Risk Management (SCRM):** Performing formal Vendor Risk Assessments (VRAs) to mathematically evaluate third-party security, privacy, and operational compliance before contracting.
2. **Contract and Legal Governance:** Executing Mutual NDAs, Teaming Agreements, Vendor Services Agreements, and Business Associate Agreements (BAAs), and managing delegations of signatory authority.
3. **Financial Transaction Processing:** Setting up vendor profiles in the Company ERP System, processing purchase orders, reconciling corporate card accounts, and executing ACH disbursements.
4. **Co-Selling and Partner Alliances:** Managing joint co-selling pipelines, tracking shared leads, and calculating sales commissions or revenue-sharing percentages.
5. **Exclusion and Debarment Compliance:** Executing mandatory monthly checks against federal registries (e.g., SAM.gov) to ensure partners and suppliers are not debarred or suspended from participating in state or federal government contracts.

5.3.2 Lawful Basis for Processing

- **Article 6(1)(f) (Legitimate Interest):** Processing B2B contact data is strictly necessary to evaluate the security, privacy, and operational resilience of our supply chain, ensuring Ready Computing protects its own infrastructure and client data from third-party vulnerabilities.
- **Article 6(1)(b) (Contract):** For executing vendor services agreements, joint alliance contracts, and processing commercial payments.

- **Article 6(1)(c) (Legal Obligation):** For complying with federal acquisition regulations (e.g., FAR Part 9 debarment screening) and corporate tax accounting standards.

5.3.3 Impact of Non-Provision

If a supplier or partner contact objects to providing the required contact, tax, or security due diligence data:

- The Company will immediately halt onboarding and refuse to execute any commercial agreements.
- The vendor cannot be registered in the Company ERP System, preventing the authorization of purchases or payment of invoices.
- The partner will be denied access to the Company Trust Center and cannot receive shared marketing leads or participate in joint co-selling campaigns.

5.3.4 Onward Transfers and Jurisdictions

Vendor and partner data is hosted within our U.S. cloud databases. Data sharing is limited to:

- The Company ERP, CRM, and contracting systems.
- Authorized third-party compliance, auditing, and GRC automation platforms.
- Corporate banking institutions.
- Federal contract auditing bodies (e.g., DCAA) when required for cost verification.

All transatlantic data transfers are covered under our active **EU-U.S. Data Privacy Framework (DPF)** and Standard Contractual Clauses (SCCs).

5.3.5 Retention Boundaries

All vendor contracts, risk assessment reports, performance scorecards, and payment ledgers are retained for exactly **seven (7) years** following the termination or expiration of the vendor or partner agreement in accordance with Company policy.

5.4 B2B Clients, Potential Clients, and Website Users

The Company collects and processes B2B commercial data, lead telemetry, and client satisfaction metrics, including:

- **Business Lead Metadata:** Contact name, corporate email address, business physical address, job title, company name, department, and professional profile links (e.g., LinkedIn).
- **Commercial Relationship and Sales Data:** Sales call notes, bid and proposal files, contract negotiation drafts, pricing tables, renewal timelines, and transaction histories.
- **Client Satisfaction (CSAT) Telemetry:** Quantitative survey responses, qualitative feedback comments, Net Promoter Scores (NPS), and account manager sentiment evaluations.
- **Website Analytics and Cookies:** IP addresses, coarsened geolocation parameters, session IDs, browser type, navigation paths, and marketing attribution data.
- **System of Record Logins:** Client user logins, usernames, and logical access logs for visualization portals.

5.4.1 Stated Purposes for Processing

Client and website visitor data is processed strictly for the following business outcomes:

1. **Client Acquisition and Sales Sourcing:** Managing the CRM pipeline, qualifying sales leads, evaluating RFP opportunities, and negotiating commercial agreements.
2. **Client Account Administration:** Executing billing, tracking project milestones in the Company ERP System, managing software subscription activations, and delivering SLA-governed support.
3. **Client Satisfaction Monitoring:** Automating quarterly CSAT surveys and monthly account manager evaluations per Company policy to detect, escalate, and remediate negative feedback.
4. **Website Optimization and Cookie Consent:** Deploying functional cookies, securing the public WordPress CMS storefront, managing opt-in preferences via our Cookiebot banner, and analyzing website traffic.
5. **Oregon-Specific Geolocation Minimization:** Enforcing precise data minimization rules for website visitors in Oregon by programmatically coarsening location tracking parameters to a radius **greater than 1,750 feet** (city level) to protect device-level privacy in accordance with state laws.

5.4.2 Lawful Basis for Processing

- **Article 6(1)(b) (Contract):** For taking pre-contractual steps at the request of a prospective client and executing Master Services Agreements, SOWs, and platform subscription agreements.
- **Article 6(1)(f) (Legitimate Interest):** For qualified sales prospecting, evaluating joint co-selling opportunities with alliance partners, administering account-management communications, and monitoring client satisfaction to prevent account churn.
- **Article 6(1)(a) (Consent):** For deploying non-essential tracking cookies and marketing scripts on our public website.

5.4.3 Impact of Non-Provision

- **Commercial Clients:** If a client contact objects to providing required administrative or billing data, the Company will be unable to draft proposals, finalize statements of work, or process commercial invoices, resulting in the termination of the business relationship.
- **Website Visitors:** If a visitor declines or ignores our Cookiebot consent banner, all analytical and marketing scripts (Google Analytics, HubSpot) remain strictly blocked, and no behavioral profiling or attribution tracking will occur.

5.4.4 Onward Transfers and Jurisdictions

All client-relationship and website telemetry data is processed on U.S.-hosted cloud servers. Dissemination is restricted to:

- Our CRM, ERP, and contracting platforms.
- Secure visualization and support ticket databases.
- The Cookiebot consent manager.
- Our cloud infrastructure providers.

Transatlantic flows are safeguarded under our active **EU-U.S. Data Privacy Framework (DPF)**, the **UK Extension**, and Standard Contractual Clauses (SCCs).

5.4.5 Retention Boundaries

- **Commercial Account Records:** All client contracts, billing invoices, CSAT metrics, and project emails are retained for exactly **seven (7) years** following the formal termination or expiration of the contract.
- **Sales Prospecting Logs:** Inbound contact details and qualified sales opportunity files are held for **three (3) years** post-opportunity closure (win/loss) per Company policy.
- **Website Tracking Analytics:** Aggregated website visitor traffic statistics and cookie preference logs are automatically deleted or expired according to the automated retention-expiry settings configured within our analytical databases.

6 INTERNATIONAL TRANSNATIONAL SAFEGUARDS

Ready Computing operates as a global enterprise with logical processing infrastructure, business processes, and workforce members situated across multiple international jurisdictions. Flows of personal data to and from countries outside the European Union (EU), the European Economic Area (EEA), and the United Kingdom (UK) are operationally necessary to support unified corporate administration, centralized payroll, global directory management, and system-wide security monitoring.

The European Commission and the UK Government have established structured legal frameworks to ensure that when personal data is transferred across international boundaries, the high level of protection guaranteed under global privacy regulations is not undermined. To establish a lawful, high-assurance pipeline for transatlantic commerce, the Company relies on active adequacy decisions and formalized cross-border transfer safeguards:

- **The EU-U.S. Data Privacy Framework (EU-U.S. DPF):** Adopted on July 10, 2023, the EU-U.S. DPF represents an adequacy decision by the European Commission, determining that the United States provides a level of personal data protection essentially equivalent to that offered within the European Union.
- **The UK Extension to the EU-U.S. DPF (UK-U.S. Data Bridge):** Effective as of October 12, 2023, the UK Extension serves as a legal determination by the UK Government that participating U.S. organizations provide adequate privacy protections for UK and Gibraltar residents under the UK GDPR.

6.1 Data Privacy Framework (DPF) Statement of Compliance

Ready Computing complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union and the United Kingdom to the United States.

The Company has formally certified to the U.S. Department of Commerce that it adheres to the Data Privacy Framework Principles (DPF Principles). This active certification was established effective as of January 2024.

If there is any conflict between the terms in this public Corporate Privacy Policy and the DPF Principles, the DPF Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view the Company's active certification record, please visit:

Official DPF Registry: https://www.dataprivacyframework.gov/

6.2 The Seven (7) Data Privacy Framework Principles

To demonstrate GRC accountability and ensure transparent processing, the Company actively enforces the seven (7) foundational DPF Principles across all internal cloud systems, product databases, and administrative operations:

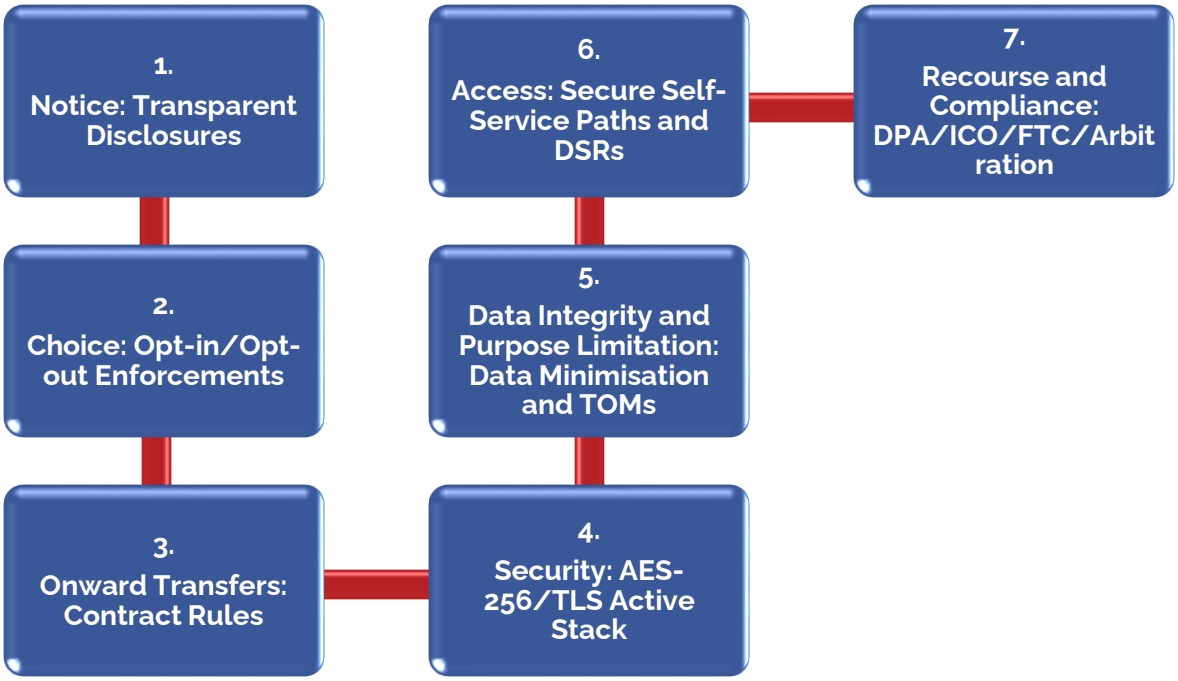

Figure 1: The Seven Principles Figure

1. **Notice:** The Company informs individuals in advance of processing regarding the categories of personal data collected, the purposes of processing, our contact details, the types of third parties to whom data is disclosed, and the available recourse paths. This principle is executed systematically via this public policy.
2. **Choice:** The Company provides clear mechanisms for individuals to opt-out if their personal data is to be disclosed to a third party or used for a purpose materially different from the purpose for which it was originally collected. For sensitive data, explicit, affirmative **opt-in consent** is obtained prior to processing.
3. **Accountability for Onward Transfer:** The Company enforces strict GRC contractual controls on any third-party agent or processor receiving personal data originating from the EU or UK. These transfers are executed strictly for specified, limited purposes under equivalent privacy protection mandates.
4. **Security:** The Company implements robust technical and organizational measures (TOMs) to secure personal data from unauthorized access, loss, or destruction. This includes **FIPS-validated AES-256 encryption at rest**, **TLS 1.3 encryption in transit**, federated identity management, and our multi-layered **workstation active defense stack**.
5. **Data Integrity and Purpose Limitation:** The Company limits personal data collection strictly to what is relevant and necessary for the specified purposes. GRC managers ensure that processed data remains accurate, complete, and current for its intended use.
6. **Access:** Data Subjects have a right to access their personal data, correct inaccurate records, and delete expired information, provided these requests do not conflict with superseding legal, tax, or provenance-preservation exemptions.
7. **Recourse, Enforcement, and Liability:** The Company has established independent recourse mechanisms to investigate and resolve unresolved DPF complaints at no cost to the individual. The

Company remains liable for damages in cases of unauthorized onward transfers of data to third-party agents.

6.3 Accountability for Onward Transfers to Agents

Ready Computing maintains overall accountability for personal data received under the DPF and subsequently transferred to a third party acting as an agent or processor on our behalf. To execute any onward transfer of personal data to a third-party subcontractor, supplier, or cloud provider, the Company enforces a structured compliance sequence:

- **Specify Limited Purpose:** Data is transferred only for limited, contractually defined purposes aligned with the original consent or lawful basis justification.
- **Impose Equivalent Protections:** The third-party recipient is contractually obligated—via an executed Data Processing Addendum (DPA) or Business Associate Agreement (BAA)—to provide at least the same level of privacy and security protection as required by the DPF Principles and applicable regulations.
- **Verification of Processing Posture:** The Company takes proactive, reasonable steps to ensure that the agent effectively processes the transferred personal data in a manner consistent with the Company's compliance obligations.
- **Failure Notification Mandate:** The contract must require the agent to immediately notify the Company if it makes a determination that it can no longer meet its obligations to provide the same level of protection required under the DPF Principles.
- **Stop and Remediate:** Upon receiving a failure notice from an agent, the Company will immediately execute its containment procedures to stop and remediate any unauthorized processing.
- **Regulatory Transparency:** The Company commits to providing a summary or a representative copy of the relevant privacy provisions of its contracts with third-party agents to the U.S. Department of Commerce or other oversight authorities upon request.

6.4 Alternative Safeguards: Standard Contractual Clauses (SCCs) and IDTAs

In scenarios where personal data is transferred internationally to a territory outside the United Kingdom or the European Economic Area that is not covered by a direct adequacy decision or DPF certification, Ready Computing enforces alternative, legally binding transfer safeguards to comply with **GDPR Article 46**:

1. **EU Standard Contractual Clauses (Commission SCCs):** For transfers of European data, the Company integrates the standardized, Commission-approved contractual clauses directly into our third-party Master Services Agreements (MSAs) and vendor contracts to guarantee equivalent protection.
2. **UK International Data Transfer Agreement (IDTA) and Addendum:** For transfers originating from the United Kingdom, the Company executes either the standalone **IDTA** or the **UK Addendum to the Commission SCCs** issued by the UK Information Commissioner's Office (ICO).
3. **Data Exporter Accountability:** Under these frameworks, the B2B Client or parent entity acts as the **Data Exporter**, and Ready Computing acts as the **Data Importer**. The Company contractually

guarantees that it maintains appropriate Technical and Organizational Measures (TOMs) to secure the transferred data per **GDPR Article 32**.

6.5 Regulatory Oversight, Recourse, and Arbitration

Ready Computing is subject to the investigative and enforcement powers of the federal regulatory and administrative bodies of the United States:

- **The Federal Trade Commission (FTC):** The FTC holds primary jurisdiction and enforcement authority over the Company's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension.
- **U.S. Department of Health and Human Services (HHS) / Office for Civil Rights (OCR):** HHS and OCR maintain overall jurisdiction and enforcement authority over the Company's compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

6.5.1 Independent Recourse for Complaints

In compliance with the DPF Principles, Ready Computing commits to resolve complaints about our collection or use of your personal information. Data Subjects with inquiries or complaints regarding our DPF compliance should first contact our central Data Protection Officer:

- **GRC Intake Channel:** privacy@readycomputing.com
- **Mailing Address:** Attn: Data Protection Officer, Ready Computing, 325 Hudson Street, Floor 4, New York, NY 10013

6.5.2 Cooperation with Data Protection Authorities (DPAs)

If a complaint cannot be resolved through the Company's internal dispute resolution and DSR appeal pathways, the Company commits to cooperate and comply with the advice of the regulatory panels established by European and UK authorities:

1. The panel established by the **EU Data Protection Authorities (DPAs)**.
2. The **United Kingdom Information Commissioner's Office (ICO)**.
3. The **Gibraltar Regulatory Authority (GRA)**.

These independent panels will investigate and resolve individual complaints brought under the DPF Principles at no cost to the individual.

6.5.3 Binding Arbitration (Annex I)

Under certain conditions, more fully described on the official Data Privacy Framework website, Data Subjects may invoke **binding arbitration** to address any complaint that has not been resolved by other recourse and enforcement mechanisms. To initiate this path, the individual must deliver formal notice to the Company and follow the procedures set forth in **Annex I** of the DPF.

APPENDICES

Appendix A: Applicable Regulatory Frameworks Directory

Ready Computing systematically maintains alignment with major global data privacy, security, and healthcare compliance frameworks. Rather than maintaining static external web links that are subject to decay, the Company maintains its operational and technical controls in alignment with the authoritative statutory bodies listed below.

Individuals, clients, and auditors may verify our active compliance status, certifications, and independent audit reports by visiting the Company's centralized online compliance portal or submitting a formal request to GRC.

International and Transnational Frameworks

- **The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679):** Governing the processing of personal data originating from the European Union and European Economic Area (EEA).
- **The United Kingdom General Data Protection Regulation (UK GDPR) / Data Protection Act 2018:** Governing the processing of personal data originating from the United Kingdom and Gibraltar.
- **The EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension:** Enabling the lawful transfer of personal data from the EU and UK to the United States under verified adequacy determinations.

United States Federal and Healthcare Frameworks

- **The Health Insurance Portability and Accountability Act (HIPAA) of 1996:** Including the HIPAA Privacy, Security, and Breach Notification Rules (45 CFR Parts 160, 162, and 164) governing Protected Health Information (PHI).
- **The Health Information Technology for Economic and Clinical Health (HITECH) Act:** Governing electronic health record security, vendor liabilities, and statutory breach notification thresholds.
- **Federal Acquisition Regulation (FAR) / Defense Federal Acquisition Regulation Supplement (DFARS):** Governing basic safeguarding of contractor information systems, subcontractor flow-down terms, and non-repudiation logging.

United States State-Level Privacy Statutes

- **The California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA):** Establishing comprehensive consumer rights, notices at collection, and data minimization rules for California residents.
- **The Washington My Health My Data Act (MHMDA):** Governing the collection, sharing, and processing of consumer health and reproductive data within the state of Washington.
- **The Nevada Consumer Health Data Privacy Law (SB 370):** Establishing strict, affirmative opt-in consent perimeters for consumer health data processed within Nevada.
- **The Oregon Consumer Privacy Act (OCPA):** Restricting the processing of precise consumer geolocation data and mandating data minimization controls.

- **The New Jersey Privacy Protection Act (NJPPA):** Governing consumer profiling, notice requirements, and strict consent rules for processing financial identifiers.

International Security and Service Standards

- **ISO/IEC 27001:2022 (Information Security Management Systems):** Serves as our primary standard for technical and administrative security controls.
- **ISO 9001:2015 (Quality Management Systems):** Serving as our master framework for quality assurance and continuous improvement.
- **ISO/IEC 20000-1:2018 (Information Technology Service Management):** Governing SLA delivery and change control boundaries.
- **HITRUST CSF Framework:** Guarantees our multi-layered endpoint and cloud environment protections meet rigorous, healthcare-vetted standards.

Appendix B: References

To ensure data integrity and prevent conflicting versions, Ready Computing does not maintain static lists of references within individual manuals.

The **Document Control Master List (DCML)** is the sole, authoritative index of all active Policies, Plans, Procedures, and Records within the Integrated Management System (IMS). Please refer to the DCML for the current version and status of all documents referenced in this document.

Appendix C: Record Retention Schedule

Ready Computing's Record Retention Schedule can be provided upon request.

Appendix D: Compliance with the DPF and its Principles

Ready Computing complies with the **EU-U.S. Data Privacy Framework (EU-U.S. DPF)** and the **UK Extension to the EU-U.S. DPF** as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data transferred from the European Union (EU) and the United Kingdom (UK) to the United States.

The Company has formally certified to the U.S. Department of Commerce's International Trade Administration (ITA) that it adheres to the **Data Privacy Framework Principles (DPF Principles)**. This certification is maintained dynamically in our centralized GRC systems to verify our ongoing compliance and ensure the seamless, lawful flow of transatlantic commercial data

Operational Integration of the Seven (7) DPF Principles

To ensure absolute GRC alignment and maintain our corporate certifications, Ready Computing systematically integrates and enforces the DPF Principles across all information lifecycles:

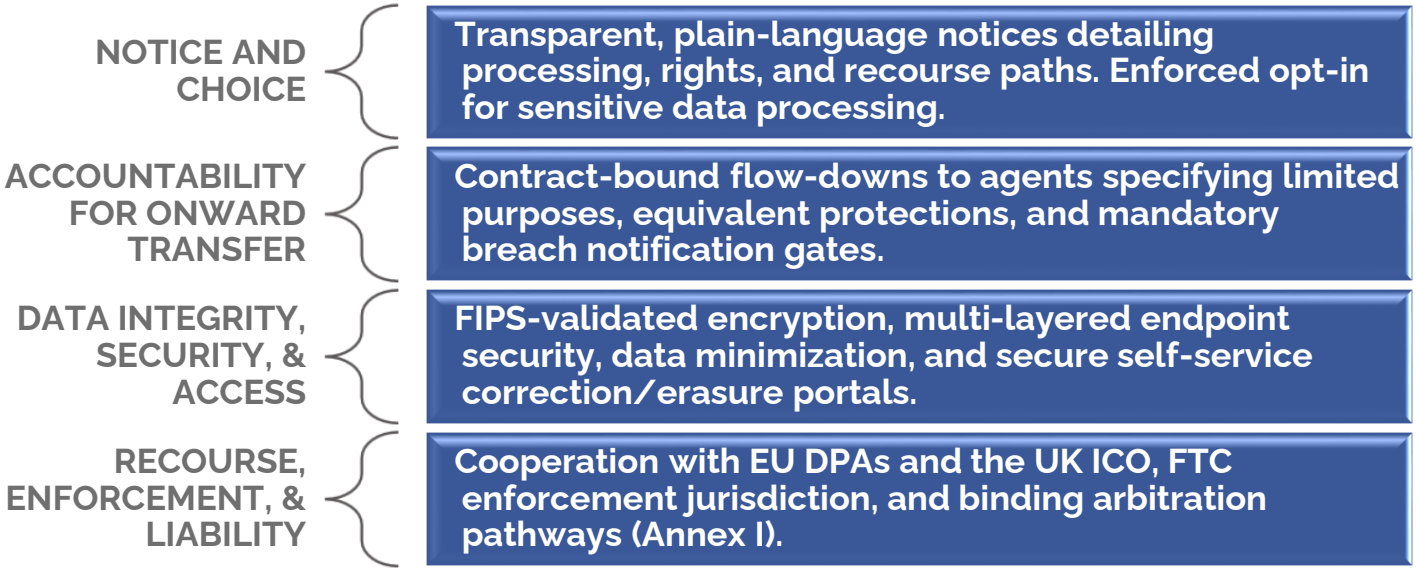

Figure 2: Operational Integration Figure

Notice

The Company transparently informs individuals about our data processing practices via this public Corporate Privacy Policy and associated notices at the point of collection. Specifically, we disclose:

- The categories of personal data we collect and process, and the specific business, regulatory, and legal purposes for which it is used.
- The independent recourse mechanisms available to investigate individual complaints at no cost, including links to the official U.S. Department of Commerce DPF website.
- The statutory rights of individuals to access their personal data under our custody.
- The requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- The specific regulatory body (the Federal Trade Commission) that has investigative and enforcement jurisdiction over our compliance with the DPF Principles.
- The Company's overall liability in cases of onward data transfers to third-party agents.

Choice

The Company respects the autonomy of data subjects and enforces robust consent management perimeters:

- Data subjects are provided with clear, accessible, and plain-language mechanisms to **opt-out** if their personal data is to be disclosed to an independent third-party controller or processed for a purpose materially different from the purpose for which it was originally collected.
- For Special Category Data—including medical records, financial identifiers, and demographic attributes—the Company programmatically enforces an **explicit, affirmative opt-in consent model**.

Processing such data is strictly blocked until the data subject proactively registers consent via our verified consent management portals.

Accountability for Onward Transfer

To transfer personal data to a third-party agent or subcontractor acting as a processor, the Company executes a structured compliance sequence to maintain data integrity:

1. **Limited and Specified Purposes:** The data is transferred strictly to perform the services defined within the corresponding contract or Statement of Work (SOW).
2. **Equivalent Protections:** The Company contractually binds the agent—via executed Data Processing Addenda (DPAs)—to provide at least the same level of privacy and security protection as required by the DPF Principles.
3. **Proactive Verification:** The Company takes reasonable and appropriate steps to ensure the agent effectively processes the transferred personal data in a manner consistent with our compliance obligations.
4. **Notification Mandate:** The agent is contractually required to notify the Company immediately if it makes a determination that it can no longer meet its obligations to provide the equivalent level of protection.
5. **Stop and Remediate:** Upon receiving a failure notice from an agent, the Company will immediately execute its incident response protocols to stop and remediate any unauthorized or non-compliant processing.
6. **Commerce Department Transparency:** The Company commits to providing a summary or a representative copy of the relevant privacy and security provisions of its contracts with third-party agents to the U.S. Department of Commerce upon request.

Security

The Company implements robust, multi-layered Technical and Organizational Measures (TOMs) to safeguard personal data against unauthorized access, alteration, loss, or destruction. This comprehensive security perimeter includes:

- **FIPS-Validated Encryption:** Enforcing AES-256 encryption for data at rest and forced TLS 1.3 encryption for data in transit.
- **Company Endpoint Defense Stack:** Programmatically locking down workstations using default-deny application control, automated operating system patching, and Next-Gen Endpoint Detection and Response (EDR).
- **Administrative Oversight:** Restricting privileged accounts to authorized personnel on a temporary, audited, and strictly peer-reviewed basis.

Data Integrity and Purpose Limitation

Ready Computing limits personal data collection strictly to what is relevant, proportional, and necessary to achieve our stated business or contractual outcomes.

- GRC managers conduct recurring audits to verify that personal data is accurate, complete, current, and reliable for its intended use.

- The Company enforces strict data minimization protocols at the intake perimeter, programmatically degrading or coarsening identifiers (such as precise geolocation data) where high-precision tracking is not legally or operationally justified.

Access

The Company respects and operationalizes the right of individuals to access their personal data:

- Data subjects may submit verified requests to privacy@readycomputing.com to confirm whether the Company is processing their personal data and to obtain a copy of their active records.
- Portals are provided to enable workforce members to securely access, correct, or update their direct profiles.
- Individuals may request the correction of inaccurate records or the deletion of expired data, subject strictly to the legal, tax, and system-provenance exemptions defined within Company policy.

Recourse, Enforcement, and Liability

Ready Computing has established robust, independent recourse pathways to ensure that any individual compliance inquiries or complaints are resolved transparently and at no cost:

1. **Internal Dispute Resolution:** Inquiries or complaints regarding transatlantic transfers should first be directed to our central Data Protection Officer (DPO) at privacy@readycomputing.com.
2. **Independent Recourse Panels:** In the event of an unresolved dispute, the Company commits to cooperate and comply with the advice of the independent regulatory panels established by:
    - The **European Union Data Protection Authorities (DPAs)**.
    - The **United Kingdom Information Commissioner's Office (ICO)**.
    - The **Gibraltar Regulatory Authority (GRA)**.
3. **FTC Enforcement:** Ready Computing's compliance with the DPF Principles is subject to the investigative and enforcement powers of the **Federal Trade Commission (FTC)**.
4. **Binding Arbitration (Annex I):** If an individual's complaint remains unresolved through our internal appeal and independent regulatory channels, they may invoke **binding arbitration** under certain conditions, as set forth in **Annex I** of the DPF, by delivering formal notice to the Company.

Maintenance and Long-Term Commitments

The Company commits to respond promptly, truthfully, and completely to all inquiries and requests for information by the ITA regarding our EU-U.S. DPF and UK Extension compliance, including during recurring re-certification audits.

Ensuring Commitments Are Kept Post-Participation

If Ready Computing decides to leave the DPF program or choose not to renew its certification:

- The Company will annually affirm to the ITA its commitment to applying the DPF Principles to all personal data received under the program for as long as such data is retained.

Alternatively, the Company will provide "adequate" protection for the retained information by other authorized means or permanently destroy/return the data in accordance with our secure sanitization standards.

Appendix E: Revision History

Revision history is maintained and can be requested.