ready COMPUTING

Solutions, Consultation, Implementation, and Managed Services

CORP POL-0008

Corporate Privacy Policy

December 2024

Version 9.0

Ready Computing
150 Beekman Street, Floor 3, New York, NY 10038 (HQ)
Moulsham Mill, Parkway Chelmsford, Essex, CM2 7PX

Certifications

TABLE OF CONTENTS

1 INTRODUCTION

Ready Computing ("Company"), is a corporate group of entities defined in 1.2 Scope, 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 in 1.5.3 Company Data Protection Officer (DPO).

1.1 Purpose

The purpose of this Privacy Policy is to provide information to all internal and external Data Subjects regarding how the Company collects personal data about Data Subjects, how it may process such data, and what rights all Data Subjects have regarding their personal data.

A secondary purpose of this Privacy Policy is to clearly communicate its commitment to all applicable frameworks, laws, regulations, and other key programs that have the purpose of protecting data and the rights of those who entrust the Company with data.

1.2 Scope

To support this purpose, Ready Computing's U.S.-based entities are structured as follows and adhere to this Policy, as well as all related Data Privacy Framework Program (DPF) Principles defined herein:

- Ready Ventures LLC (i.e., parent, holding company)
  - Ready Computing Resources LLC
    - Ready Computing Government Solutions LLC
    - Ready Computing Commercial Solutions LLC
    - Ready Computing Innovations LLC
    - Ready Computing Limited

1.2.1 Regulatory Scope

Ready Computing is an international organization that complies with the Health Insurance Portability and Accountability Act (HIPAA), U.S. Data Privacy Laws (e.g., CCPA/CCPR, etc.), and the EU/UK GDPR. Ready Computing is assessed by certified third-party auditors on an annual-basis to demonstrate its compliance. You may send a request for a copy of any of our audits to the Company contact listed in 1.5.3 Company Data Protection Officer (DPO). Your request will be reviewed and responded to within 30-days.

1.2.2 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 C: Compliance with the DPF and its Principles for additional information.

- United States Data Privacy Laws (i.e., All states)
  - Please refer to Appendix A: References and Sources for references and sources.
- United States HIPAA

1.3 Audience

The primary audience of this Policy is all Data Subjects, both internal and external, as well as all Personnel who have any responsibilities in the creation, maintenance, or execution of this Policy.

An additional audience for this document is all third-party auditors, assessors, and other interested parties ensuring that the Company is actively complying with the framework, laws, and regulations it claims to.

1.4 General Information

The information in this section is relevant to all categories of Data Subjects.

1.4.1 Who Controls Personal Data?

- Ready Computing is responsible for personal data.

1.4.2 General Company Contact Information

- privacy@readycomputing.com

1.4.3 Company Data Protection Officer (DPO)

- Ready Computing has appointed its Director of Compliance and Risk Management as its DPO.
  - This role's email contact information is as follows: Data Protection Officer

1.4.4 Company Privacy and Security Officer

- Ready Computing has appointed its CISO, as its Privacy and Security Officer (PSO).
  - This role's email contact information is as follows: Privacy and Security Officer

1.4.5 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.

1.4.6 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.

1.4.7 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

All employees, contractors, and vendors (as defined by Ready Computing's Vendor Management Policy) will receive training and awareness, as follows:

- External Online Training (i.e., e-learning through a System)
- Internal Online Training (i.e., e-learning created internally)
- Documentation Training (i.e., this document, and others related to it)
- On the Job (OJT) Training (i.e., select Personnel may receive a higher degree of training)

1.5.1 Intervals of Training

Training will occur on at least one of the following intervals:

- During onboarding and annually, every calendar year thereafter.
- As-needed, when material changes to Company Documentation or Programs occur.

1.5.2 Reporting

All records are generated and maintained in the Company's Human Resources Management System (HRMS) and audited monthly. These statistics are reported to the Executive Team monthly.

1.6 Confidentiality Statement

The information contained within this document is intended for "Public" use, as defined by *Data Classification and Risk-Based Controls Policy*.

2 CORPORATE PRIVACY PROGRAM OVERVIEW

The Company processes Data Subject's personal data for various purposes. Personal data involves data that comes from Company Personnel and Clients. This Corporate Privacy Policy incorporates controls to adhere and comply with the GDPR, U.S. Privacy Law, and the DPF. This includes the seven (7) Data Protection Principles defined in the GDPR:

2.1 Seven (7) Data Protection Principles

2.1.1 Lawfulness, Fairness and Transparency

The Company ensures:

- Data processing meets the criteria outlined in the GDPR for:
  - Consent
  - Contract
  - Legal Obligation
  - Vital Interest
  - Public Task; or
  - Legitimate Interest
- Data processing matches the description given to the Data Subject (DS) in thie Privacy Policy, and is being used only for the purposes and time indicated.
- Clear communication is provided regarding the nature of any DS Data Processing.

2.1.2 Purpose Limitation

The Company only processes a Data Subject's data (whether directly or indirectly) for a legitimate, legal reason. The Company cannot state that it is processing data for one reason and then use it for another without first informing the Data Subject.

2.1.3 Data Minimisation

The Company only collects the minimum amount of personal data for the stated purpose.

2.1.4 Accuracy

The Company ensures that the personal data processed is accurate and is kept current.

2.1.5 Storage Limitation

The Company only retains personal data for as long as the intended legitimate purpose requires it to be held. Afterwards this data is deleted in accordance with its *Data Retention Policy*.

2.1.6 Integrity and Confidentiality

The Company ensures that all personal data is held securely, using suitable, up-to-date security measures. For most modern data processing, this means that suitable and current cybersecurity measures have been

implemented as controls in accordance with published Information Security Management System (ISMS) Policies that have been certified to the ISO/IEC 27001:2022 Standard.

2.1.7 Accountability

The Company is legally accountable for upholding all seven (7) principles and demonstrates compliance through internal and external auditing.

2.1.8 Records and Evidence

The GDPR and U.S. Privacy Law provides guidance on how to best protect personal data and the rights of Data Subjects. To comply, specific documents have been created and are maintained. Here is a brief overview and description of each of the major Corporate Privacy Program Documentation inputs.

2.1.8.1 Corporate Privacy Policy (i.e., this Policy)

This document is synonymous with "Privacy Notice." Articles 12, 13, and 14 of the GDPR, and each U.S. State with applicable laws, provides guidance and legal requirements for how to best create, implement, and maintain a Privacy Notice. This is a "Public" document that explains how personal data is processed, the rights a Data Subject has, and how the Company applies data protection principles. Navigate to Appendix B: Record Retention Schedule for more information.

2.1.8.2 Record of Processing Activities (RoPA)

Article 30 of the GDPR stipulates the need for data controllers to create and maintain a Record of Processing. This record is a document with the purpose of creating an inventory of data processing activities that can be analyzed to help the Company precisely identify:

- Controllers, Processors, and Joint Controller.
- Categories of processed data.
- Why data is being processed and what is being done with it.
- Who has access to, or are the recipients of the personal data.
- Data Retention Schedules
- TOMs, or other controls that have been implemented to protect data.
- If special category data is being processed.

For a complete list of RoPA, please make a request by contacting the Company Contact identified in section 1.5.3 of this Policy.

2.1.8.3 Data Protection Impact Assessments (DPIAs)

A DPIA is a process to help identify and minimize data protection risks. DPIAs are conducted when:

- There is a potential high level of risk to the rights and freedoms of a data subject.
- There is a major project involving the use of personal data or the project uses automated decision-making or systematic monitoring.
- Sensitive data or data of a highly personal nature is processed.

- Data is processed on a large scale or data concerning vulnerable data subjects, such as children or criminals, is being processed.

There may be instances that the Company chooses not to conduct a DPIA. This is a decision that must be made by the DPO and approved by the Executive Team. DPIAs can be requested by contacting the DPO.

2.1.8.4 Record Retention and Disposal

The Company maintains a Record Retention and Disposal Schedule that provides a comprehensive list of all types of records, data, and information that must be retained, and for what period. Please refer to Appendix B: Record Retention Schedule for more information.

2.2 Audits

The Corporate Privacy Program will be audited on an annual-basis in the following ways:

2.2.1 Internal Audits

Internal audits are conducted continuously and on an established schedule.

2.2.2 External Audits

External Audits are audits that are independently performed by a third-party. The Company will evaluate the need for an external audit on an annual-basis, or when a variable is introduced that may necessitate the need for an external evaluation.

3 DATA SUBJECT'S RIGHTS

The GDPR and U.S. State Privacy Laws provides the following rights for Data Subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

3.1 The Right to be Informed

Data Subjects have the right to be informed about how the Company processes personal data. Typically, the Company communicates this information through a privacy policy, such as this one.

3.2 The Right of Data Access

Data Subjects have a right to obtain a copy of the personal data the Company retains, subject to certain exceptions.

3.3 The Right of Data Rectification

Data Subjects always have a right to ask for an immediate correction of inaccurate or incomplete personal data that the Company retains related to the Data Subject.

3.4 The Right of Data Erasure

- Data Subjects have the right to request that personal data be erased when it is no longer needed, and where applicable law obliges the Company to delete the data or cease the processing of it due to its unlawfulness.
- Data Subjects may also ask the Company to erase personal data when consent has been withdrawn or a Data Subject objected to the data processing. However, this is not a general right to data erasure and there are exceptions.

3.5 The Right to Restrict Data Processing

Data Subjects have the right to restrict the processing of personal data in specific circumstances. Where that is the case, the Company may still store your information, but not use it further.

3.6 The Right to Data Portability

Data Subjects have the right to receive their personal data in a structured, machine-readable format, or to request the Company to share it with a third-party.

3.7 The Right to Object to Data Processing

Data Subjects have the right to object to the Company's processing of their personal data based on the legitimate interests; where their data privacy rights outweigh the Company's reasoning for legitimate interests.

3.8 Rights in Relation to Automated Decision Making and Profiling

- Data Subjects have the right to not be subjected to a decision based solely on automated processing which produces legal or similarly significant effects. This includes profiling. Currently, the Company does not perform any automated decision making or profiling.
- Data Subjects may request to enforce their data privacy rights by emailing the Company-appointed DPO at the email address provided in section 1.5.3 of this document.
- In certain circumstances, the Company may need to restrict the above rights to safeguard public interest (e.g., the prevention or detection of crime) or our business interests (e.g., the maintenance of legal privilege).

3.9 Data Subject Requests (DSRs)

It is this Company's commitment to ensure all Data Subjects that interact with the Company have received, understand, and can execute their rights against this Policy.

- A DSR can be made to any Company Personnel, at any time, and in any format. The DSR does not have to be requested in a specific way, nor does it have to use specific language. DSRs must be submitted to the DPO without delay.
- Once submitted, it is the duty of the DPO to manage the DSR until it is closed. It is the DPOs responsibility to respond to all DSRs within 30 days of submission. The DPO may request assistance from specific Personnel at any time for assistance in completing this request. To comply, the Company DPO has created and manages a Data Subject Request Log.

4 GENERAL INFORMATION

As a Data Subject, you maintain certain rights that the Company has obligations to observe. The following section of this document provides a complete outline of all the pertinent information that Data Subjects have a right to.

4.1 Consent as a Legal Basis for Processing

For some data processing, the Company uses consent as a legal basis. If a Data Subject has consented to processing by the Company, please be aware that a Data Subject has the right to withdraw this consent at any point. To withdraw consent for a particular type of data processing that the Company performs, you may contact the to the Company Contact identified in section 1.5.3 of this Policy.

4.2 Complaints to a Supervisory Authority

Data Subjects have the right to lodge a complaint with a "supervisory authority" (UK/EU) or applicable Department of Justice (U.S.) with regards to the way that the Company processes personal data. If a UK/EU Data Subject would like to submit a complaint, the Company recommends lodging a complaint with the Information Commissioner's Office (ICO). This is the UK's supervisory authority and is the one which the Company is registered with. If the Data Subject is a U.S. Citizen, then that Data Subject should file a complaint with the appropriate Department of Justice relevant to the State in which they would like to cite their complaint.

4.3 How the Company Shares Your Data

The Company will not share your information with any third parties for the purposes of direct marketing, and will not sell your data.

The Company uses data processors who are third parties who provide elements of services. For those services, the Company has contracts in place with the data processors. This means that they cannot do anything with a Data Subjects personal information unless we have instructed them to do it. Third parties will not share your personal information with any organization apart from the Company, unless it has been authorized by the Company. Third parties will hold it securely and retain it for the period the Company instructs.

In some circumstances, the Company is legally obligated to share information (e.g., a court order). In a scenario such as this, the Company will document that we have a lawful/legal basis on which to share the information.

4.3.1 Transfers of Personal Data

As of July 10, 2023, the EU-US DPF was adopted and the U.S. was given an adequacy decision. Additionally, in effect as of October 12, 2023, is the UK Extension to the EU-U.S. DPF (i.e., UK-U.S. Data Bridge). This essentially is defined as a legal determination by the European Commissions that the U.S. provides a level of personal data protection offered within the EU under the GDPR.

Ready Computing is an international organization with entities in the UK and the US. It is possible that over the course of business activities, the Company may transfer your personal data to third-party, cloud based, storage systems and/or financial management systems. The Company will ensure that personal data is

hosted in UK/EU and US servers. Transfers to U.S. third-parties will only be to commercial organizations participating in the EU/UK-US Data Privacy Framework. The Company will ensure that contracts with these third parties meet all UK/EU GDPR requirements. The Company only transfers personal data to territories who have been given an adequacy status.

4.4 How the Company Protects Your Information

The Company has implemented appropriate technical and organizational measures (TOMs) and data security controls to protect personal data that the Company retains. These controls and measures will help to sustainably mitigate unauthorized disclosure of personal data, as well as any unauthorized use, alteration, or destruction of it. Where appropriate, the Company uses encryption and other technologies that assist in securing data. It is also a requirement that our service providers comply with strict data privacy requirements where they process personal data.

4.5 How Long Will the Company Retain Personal Data?

The Company only retains personal data for as long as necessary and for the purposes described in this privacy policy; or until a Data Subject notifies the Company to cease processing data. After this time, the Company will securely delete personal data, unless there is a legitimate reason to keep it, to meet legal or regulatory obligations, or to resolve potential legal disputes.

4.6 Contact and Further Information

- If you have any questions about how the Company uses personal data, or if you wish to submit a complaint about how the Company handles it, you may contact the to the Company Contact identified in section 1.5.3 of this Policy.
    - If you would like to be provided with information about a specific personal data processing activity, you can request that by submitting a request to the Company Contact identified in section 1.5.3 of this Policy.
- The Company only collects personal data it needs for the purposes described above. Certain personal data collected from Data Subjects relates to your next of kin and emergency contacts. In these cases, you are requested to inform such persons about this Policy.
- If you are working at a third-party site (e.g., a Company customer location or facility), such third party may need to process personal data for their purposes acting as a data controller. In these cases, you may request a separate privacy notice/policy from the relevant data controller.

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

5.1.1 Standard Types of Information the Company Collects and Uses

The Company collects and uses personal data that concerns you in connection with your employment. The Company may collect the following categories of personal data:

- Personal details and identification data such as name, personal and business address, personal and business telephone number, personal and business email address or any other contact details, date, and country of birth.
- Personal data related to family and social circumstances such as gender, age, marital and family status (including the name and contact details of the next of kin).
- Employment related personal data such as: signature, employment status, national insurance numbers, insurance number, country of residence, nationality, photo, emergency contacts, passport information, work and residence permit, immigration status and travel visa information.
- Qualifications such as qualifications and certifications including current and previous positions, education and training courses, resume/CV, records of education and work achievements, in some cases: contact details of referees and results of capability assessments and interview assessment/feedback.
- Job information and work metrics such as position, title, employment contract, payroll ID, line manager, job band, performance history, employment status, leave of absence information, working time logging, training records, performance targets and development goals. In some cases, the Company may also record results of capability assessments, safety reports and incidents, and professional feedback.
- Compensation, allowances, benefits, and expense related information such as salary data, payroll data, pension plan number and contributions, non-salary benefits, bonus, compensation, share options, dependents, beneficiaries or health benefit nomination, bank statements, expense claims and receipts, bank account details, credit card data, phone expenses and insurance data.
- Electronic identification data and information (where employee has access or is affected by such systems or applications) such as access logs, IT and internet usage, device identifiers (mobile device ID, PC ID etc.), registration and login credentials, IP address, tracking and analytics data, recordings (e.g., voice mail/call recordings), posts on corporate platforms (e.g., Yammer), password recovery data, information obtained via IT security tools.
- Financial and other details such as account information, credit checks, payment details and transactions, investigation information and disciplinary history.

- Other personal data (which may include special categories of information as mentioned below) namely where you or others (such as your colleagues) may register these data on or in our systems, programs, and application such as business documents containing personal information (e.g., queries, questions, complaints, orders, and related records; emails; reports; contracts; presentations, minutes; work products), photos, images and/or videos.

5.1.2 Special Categories of Personal Data

The below mentioned types of personal data are only collected and processed, if at all, in accordance with applicable local laws in your country of residence.

- Membership of religious congregations (e.g., if required for tax purposes);
- Health and medical information, including, but not limited to:
    - Reproductive health information
    - Medical procedures
    - Disability status
    - Special working conditions (such as use of a standing desk) and medical devices needed on the premises
    - Work related injury and illness information
    - Data for travel emergency support (blood type, medical history, allergies);
- Race or ethnicity (e.g., where this is used for diversity purposes);
- In some cases: trade union membership, political opinions and sex life or sexual orientation (e.g., where this is used for investigations of non-equal treatment).
- Data about criminal convictions and offences such as criminal background information and sanction list information to the extent required for the purposes of criminal background screening and Know Your Customer and Anti Money Laundering obligations.
- To the extent necessary to fulfil our obligations, data obtained from publicly accessible sources or which are legitimately transmitted by other third parties (e.g., a credit agency) such as data in public professional social media (e.g., LinkedIn), background check data.

In case you would like to be provided with information about a specific personal data processing activity, you can request that by submitting a request to the Company Contact identified in section 1.4.3 of this Policy.

5.1.3 Use of Data

The company may use your personal data as listed above for the following purposes:

- Human resources management including organization and personal administration, working hours management, improving, and maintaining effective staff administration, internal workforce analysis, reporting and planning;
- Staff transfer management from different affiliates and succession planning;

- Payroll, compensation, and benefits management including providing staff benefits and maintaining salary, compensations including intellectual property, allowances, benefits, insurances, pensions, and performance reviews;
- Talent management and acquisition including recruitment, assessing suitability, and working capacity, background checks and verification of qualifications, obtaining and providing references;
- Learning and development management including certifications, training staff, and performing assessments and employee satisfaction surveys;
- Processes related to joining and leaving including internal moves and terminations;
- Sickness and other leave and vacations management;
- Internal health and safety programs including health and safety and accident records or reporting and managing process quality;
- Travel and expenses management and organization of business trips including monitoring of travelers to provide support during security or medical emergencies; providing travel security, health and safety training and on voluntary basis assistance in giving security support during emergencies;
- Carrying out the obligations and exercising specific rights in the field of employment or a collective agreement;
- Internal and external communication of the Company's organization and representation of the Company including commercial register and assigning powers of attorney;
- Organizing Company events and documentation of such events including managing and organizing internal non-marketing related campaigns, events, and meetings;
- Managing Company assets including pictures and videos depicting employees or other individuals available for download on the Company intranet, the Company website, etc.;
- Finance and shared accounting services providing record to report, order to cash and purchase to pay services;
- Reorganization, acquisition and sale of activities, business units and companies;
- Business reporting, statistics, and analytics;
- Monitoring and auditing compliance of employees' activities in the workplace with the Company's corporate policies, contractual obligations and legal requirements including disciplinary actions;
- Carrying out audits, reviews, and regulatory checks to meet obligations to regulators;
- Governance, risk and compliance, including compliance with laws, law enforcement, court and regulatory bodies' requirements (such as for the process of verifying the identity of customers, called as Know Your Customer / Anti Money Laundering monitoring purposes), customs and global trade compliance, conflict of interest and security obligations) and prevention, detection, investigation and remediation of crime and fraud or prohibited activities or to otherwise protect legal rights and to establish, exercise or defend legal claims;

- Managing the customer relationship, processing customer orders, and providing customer support, processing, evaluating, and responding to requests and inquiries;
- Managing the suppliers, contractors, advisers, and other professional experts including contact interaction, processing, and fulfilling purchases and invoices, and contract lifecycle management;
- Making use of work performance and products and for references on documents, such as drawings, purchase orders, sales orders, invoices, reports;
- Access control system providing electronically controlled ingress and/or egress for authorized individuals to locations that have access restrictions and a registry of personnel on site in case of emergencies;
- Intrusion detection including 3rd party monitoring of duress, perimeter, internal security points and ancillary supervisory monitors for site maintenance/automated systems;
- Maintaining and protecting the security of products, facilities, services, systems, networks, computers, and information, preventing, and detecting security threats, fraud or other criminal or malicious activities, and ensuring business continuity; and
- Managing IT resources, including infrastructure management including data back-up, information systems' support and service operations for application management, end user support, testing, maintenance, security (incident response, risk, vulnerability, breach response), master data and workplace including user accounts management, software licenses assignment, security and performance testing and business continuity.

The Company only collects the personal data from you that it needs for the purposes described above. Certain personal data collected from you relates to your next of kin and emergency contacts. In these cases, you are requested to inform such persons about this Notice.

In case you are working at a third-party site (for example a Company customer location or facility), such third party may need to process your personal data for their purposes acting as a data controller. In these cases, you will receive or may request a separate privacy notice from the relevant data controller.

5.1.4 When an Information Request is Refused by the Data Subject

Where it concerns processing operations related to your employment (as described above), the Company will not be able to adequately employ you without certain personal data and you may not be able to exercise your employee rights if you do not provide the personal data requested. Although the Company cannot mandate you to share your personal data with us, please note that this then may have consequences which could affect your employment in a negative manner, such as not being able to exercise your statutory rights or even to continue your employment. Whenever you are asked to provide us with any personal data related to you, the Company will indicate which personal data is required, and which personal data may be provided voluntarily.

5.1.5 Legal Basis

For the use of your personal data for the purposes described above (in section 4), the Company relies on the following legal basis, as applicable:

- The Company processes your personal data for the fulfilment of obligations in your employment contract with us and similar collective employment agreements, or as part of pre-contractual measures to establish employment and related contracts;
- In some cases, the Company relies on our legitimate interests to process your personal data insofar as this is not overridden by your own privacy interests. Such interests may include:
    - Monitoring (for example through IT systems), investigating and ensuring compliance with legal, regulatory, standard and the Company internal requirements and policies;
    - Prevention of fraud and criminal activity including investigations of such activity, misuse of Company assets, products, and services, and as strictly necessary and proportionate for ensuring network and information security; and
    - Transmitting personal data within the Company group for internal administrative purposes as necessary, for example to provide centralized services.
- You may obtain a copy of our assessment regarding our legitimate interest to process your personal data by submitting a request to the Company Contact identified in section 1.5.3 of this Policy.
- In some cases, the Company processes your personal data based on statutory requirements, for example, based on labor law, allowances, tax or reporting obligations, cooperation obligations with authorities or statutory retention periods to carry out our contractual responsibilities as an employer;
- In exceptional circumstances the Company may ask your consent at the time of collecting the personal data, for example photos, communications materials, and events. If the Company ask you for consent to use your personal data for a particular purpose, the Company will remind you that you are free to withdraw your consent at any time and the Company will tell you how you can do this.

5.1.6 Special Categories of Personal Data

The Company will only process such data in accordance with applicable law and:

- With your explicit consent for specific activities in accordance with applicable law;
- When necessary for exercising rights based on employment, or social protection law or as authorized by collective agreement, or for preventive and occupational medicine or and evaluation of working abilities; or
- Where necessary for establishment, exercise, and defense of legal claims.

Regarding personal data concerning criminal convictions and offences, the Company will only process such data where such processing is permitted by applicable (local) law.

5.2 Contractors, Potential Contractors, or Service Contract Workers

5.2.1 Standard Types of Information the Company Collects and Uses

The Company collects and uses personal data that concerns you in connection with your work assignment and the services you are providing under the work assignment/statement of work directly to the Company. The Company may collect the following categories of personal data:

- Identification data and business contact information, you share with us such as first name, last name, job/position/title, employer, employer address, nationality, tax number, work permit/visa information, business email address, business address, telephone number, mobile telephone number, telefax number, private telephone number, private email address, gender, date of birth.
- Additional information you provide to us in the course of your work assignment such as data concerning the fulfilment of your work assignment, our contractual obligations and pre-contractual measures including correspondence data, offers, tenders, resume/CV, background check data, conditions, qualifications/certificates, contract and order data, invoices, payments, business partner history, records relating to queries/questions/complaints/orders, working time logging, and training and education records, vehicle license plate, insurance data.
- Expense related information such as bank statements, payment details, transactions, expense claims and receipts, bank account details, credit card data.
- Electronic identification data and information collected by the communications systems, IT applications and website browser (where contractor has access or is affected by such systems or applications and in accordance with the applicable law) such as information technology usage (system access, IT and internet usage), device identifier (mobile device ID, PC ID), registration and login credentials, IP address, login data and log files, Analytics ID, digital alias/signature, time and URL, searches, website registration and cookie data recordings (e.g., voice mail/phone recordings, Skype recordings).
- Other personal data namely where you or others (such as your colleagues) may register these data on or in our systems, programs, and application such as business documents containing personal information (e.g., queries, questions, complaints, orders and related records, emails, reports, contracts, presentations, minutes, work products).
- Photos, images, and/or videos.

The below mentioned types of personal data are only collected and processed, if at all, in accordance with applicable local laws in your country of residence and where relevant depending on your work assignment.

- Special categories of personal data such as data for travel emergency support (blood type, medical history, allergies).
- Data about criminal convictions and offences such as criminal background information for the purposes of criminal background screening.
- To the extent necessary to fulfil our obligations, data obtained from publicly accessible sources or which are legitimately transmitted by other third parties (e.g., a credit agency) such as data transferred to the Company by your employer or the company through which you are assigned to the Company, commercial register data, creditworthiness data.

In case you would like to be provided with information about a specific personal data processing activity, you can request that by submitting a request to the Company Contact identified in section 1.5.3 of this Policy.

5.2.2 Use of Data

The Company may use your personal data as described above for the following purposes:

- Human resources management as relevant to your work assignment and the services you are providing under the work assignment/statement of work directly to the Company including organization and personal administration, working hours management, improving, and maintaining effective staff administration, internal workforce analysis, reporting and planning;
- Supplier and service provider management throughout the procurement, logistics and supply chain including contact interaction including tendering, engagement, processing orders, process and fulfilment of purchases, administration and management of suppliers, vendors, contractors, advisers, and other professional experts including contact interaction, processing, and fulfilling purchases and invoices, and contract lifecycle management;
- Staff transfer management from different affiliates and succession planning;
- Training contractors;
- Internal health and safety programs;
- Travel and expenses management and organization of business trips including monitoring of travelers to provide support during security or medical emergencies, providing travel security, health and safety training and on a voluntary basis assistance in giving security support during emergencies, insurance management;
- Finance and shared accounting services providing record to report, order to cash and purchase to pay services;
- Making use of work performance and products and for references on documents, such as drawings, purchase orders, sales orders, invoices, reports;
- Reorganization, acquisition and sale of activities, business units and companies;
- Monitoring and auditing compliance with the Company's corporate policies, contractual obligations, and legal requirements;
- Carrying out audits, reviews, and regulatory checks to meet obligations to regulators;
- Maintaining and protecting the security of products, facilities, services, systems, networks, computers, and information, preventing and detecting security threats, fraud or other criminal or malicious activities, and ensuring business continuity; and
- Managing IT resources, including infrastructure management including data back-up, information systems' support and service operations for application management, end user support, testing, maintenance, security (incident response, risk, vulnerability, breach response), master data and workplace including user accounts management, software licenses assignment, security and performance testing and business continuity.

The Company only collects the personal data from you that it needs for the purposes described above. For statistical purposes, improvement of our services and testing of our IT systems the Company uses as much anonymized data as reasonably possible. This means that these data can no longer (in)directly identify you or single you out as an individual.

5.2.3 When an Information Request is Refused by the Data Subject

Where it concerns processing operations related to your work assignment (as described above), the Company will not be able to adequately establish, conduct or terminate a business relationship with you, your employer, or the company through which you are assigned to the Company and generally perform the purposes described above without certain personal data. Although the Company cannot obligate you to share your personal data with us, please note that this then may have consequences which could affect your work assignment in a negative manner, such as not being able to take requested pre-contractual measures to enter a contract with you, your employer, or the company through which you are assigned to the Company or to establish and continue your work assignment.

5.2.4 Legal Basis

The Company uses your personal data for the purposes described in this notice based on one of the following legal bases, as applicable:

- The Company may process your personal data for the fulfilment of contractual obligations resulting from your work assignment, or as part of pre-contractual measures the Company take;
- In some cases, the Company rely on our legitimate interests to process your personal data insofar as this is not overridden by your own privacy interests. Such interests may include:
    - Conduct, management, development, and furtherance of our business in the broadest sense possible including supply of products and services, performance of agreements and order management with suppliers, process and fulfilment of purchases, process quality management and improvement of products or services, analytics and market intelligence, reduction of default risks in our procurement processes and reorganization, acquisition and sale of activities, business divisions and companies;
    - Monitor, investigate and ensure compliance with legal, regulatory, standard and the Company internal requirements and policies;
    - Prevent fraud and criminal activity including investigations of such activity, misuse of Company assets, products, and services, and as strictly necessary and proportionate for ensuring network and information security; and
    - Transmitting personal data within the Company group for internal administrative purposes as necessary for example to provide centralized services.

You may obtain a copy of our assessment of why the Company may process your personal data for these interests by submitting a request to the Company Contact identified in section 1.5.3 of this Policy.

In some cases, the Company processes your personal data based on legal obligations and statutory requirements, for example, based on tax or reporting obligations, cooperation obligations with authorities, statutory retention periods or the disclosure of personal data within the scope of official or judicial measures may be required for the purposes of taking evidence, prosecution, or enforcement of civil law claims.

5.2.5 Special Categories of Personal Data

- The Company will ask your explicit consent for specific activities in accordance with applicable law; or
- Where necessary for establishment, exercise, and defense of legal claims.

Regarding personal data concerning criminal convictions and offences, the Company will only process such data where such processing is permitted by applicable (local) law.

5.3 Vendors (i.e., Suppliers or Potential Suppliers)

The Company collects and uses personal data in connection with the agreements with our suppliers. The Company may collect the following categories of personal data:

- Identification data and business contact information, you share with us such as first name, last name, job/position/title, nationality, business email address, business address, telephone number, mobile telephone number, telefax number, private telephone number, gender, date of birth.
- Additional information you provide to us during our business relations such as data concerning the fulfilment of our contractual obligations and pre-contractual measures including correspondence data, offers, tenders, resume/CV, conditions, contract and order data, invoices, payments, business partner history, records relating to queries/questions/complaints/orders.
- Electronic identification data and information collected by the communications systems, IT applications and website browser (where supplier has access or is affected by such systems or applications and in accordance with the applicable law) such as information technology usage (system access, IT and internet usage), device identifier (mobile device ID, PC ID), registration and login credentials, IP address, login data and log files, Analytics ID, time and URL, searches, website registration and cookie data, sound recordings (e.g., voice mail/phone recordings, Skype recordings).

The below mentioned types of personal data are only collected and processed, if at all, in accordance with applicable local laws in your country of residence and where relevant depending on the agreements with our suppliers.

- Data about criminal convictions and offences such as criminal background information and sanction list information to the extent required for the purposes of criminal background screening, due diligence, and Anti Money Laundering obligations
- To the extent necessary to fulfil our obligations, data obtained from publicly accessible sources or which are legitimately transmitted by other third parties (e.g., a credit agency) such as commercial register data, creditworthiness data.

5.3.1 Use of Data

The Company may use your personal data as described above for the following purposes:

- Supplier and service provider management throughout the supply chain including contact interaction including tendering, engagement, processing orders, process and fulfilment of

purchases, administration and management of suppliers, vendors, contractors, advisers, and other professional experts;

- Paying debts, supplier invoice and payment management, purchasing of direct and indirect services;
- Reporting and analytics including market intelligence and development and improvement of services or products through assessment and analysis of the information;
- Management of process quality;
- References on documents, such as tenders, purchase orders, invoices, reports;
- Contract lifecycle management;
- Payment collection and insolvency processes;
- Training suppliers;
- Finance and shared accounting services, providing record to report and purchase to pay services;
- Reorganization, acquisition and sale of activities, business units and companies;
- Monitoring and auditing compliance with the company's corporate policies, contractual obligations, and legal requirements;
- Carrying out audits, reviews, and regulatory checks to meet obligations to regulators;
- Governance, risk, and compliance, including due diligence and anti-money laundering obligations, customs and global trade compliance and sanctioned party list screening, security, including prevention, detection of crime and fraud;
- Maintain and protect the security of products, facilities, services, systems, networks, computers, and information, preventing and detecting security threats, and fraud or other criminal or malicious activities; and
- Manage IT resources, including infrastructure management including data back-up, information systems' support and service operations for application management, end user support, testing, maintenance, security (incident response, risk, vulnerability, breach response), user accounts management, software licenses assignment, security and performance testing and business continuity.

The Company only collects the personal data from you that it needs for the purposes described above. For statistical purposes, improvement of our services and testing of our IT systems the Company uses as much anonymized data as reasonably possible. This means that these data can no longer (in)directly identify you or single you out as an individual.

5.3.2 When an Information Request is Refused by the Data Subject

Where it concerns processing operations related to the agreements with our suppliers (as described above), the Company will not be able to adequately establish, conduct or terminate a business relationship with you or your company and generally perform the purposes described above without certain personal data. Although the Company cannot obligate you to share your personal data with us, please note that this then may have consequences which could affect the business relationship in a negative manner, such as not

being able to take requested pre-contractual measures to enter a contract with you or to establish and continue the business relationship you have asked for.

5.3.3 Legal Basis

The Company uses your personal data for the purposes described in this notice based on one of the following legal bases, as applicable:

The Company may process your personal data for the fulfilment of contractual obligations resulting from contracts with you or your company, or as part of pre-contractual measures the Company take;

In some cases, the Company rely on our legitimate interests to process your personal data insofar as this is not overridden by your own privacy interests. Such interests may include:

- Conduct, management, development, and furtherance of business in the broadest sense possible including supply of products and services, performance of agreements and order management with suppliers, process and fulfilment of purchases, process quality management and improvement of products or services, analytics and market intelligence, reduction of default risks in our procurement processes and reorganization, acquisition and sale of activities, business divisions and companies;
- Monitor, investigate and ensure compliance with legal, regulatory, standard and the Company internal requirements and policies;
- Prevent fraud and criminal activity including investigations of such activity, misuse of Company assets, products and services, and as strictly necessary and proportionate for ensuring network and information security; and
- Transmitting personal data within the Company group for internal administrative purposes as necessary for example to provide centralized services.

In some cases, the Company processes your personal data based on legal obligations and statutory requirements, for example, based on tax or reporting obligations, cooperation obligations with authorities, statutory retention periods or the disclosure of personal data within the scope of official or judicial measures may be required for the purposes of taking evidence, prosecution, or enforcement of civil law claims.

Regarding personal data concerning criminal convictions and offences, the Company will only process such data where such processing is permitted by applicable (local) law.

5.4 Clients or Potential Clients

5.4.1 Standard Types of Information that the Company Collects and Uses

The Company collect the following categories of personal data:

- The business contact information you share with us: name, title, job title, email address, business address, telephone number, mobile telephone number
- Additional information you provide to us during our business relations, such as: interests in the Company services or products, marketing preferences, registration information provided at events, fairs, contract or order data, invoices, payments, business partner history, etc.

- Information your browser makes available when you visit the Company website: IP address, the source of your site visit, time spent on the website or a particular page, links clicked, comments shared, browser type, date, and time of visit, etc.
- To the extent necessary to fulfil our obligations, data obtained from publicly accessible sources or which are legitimately transmitted by other third parties (e.g., a credit agency): commercial register data, association register data, creditworthiness data.

5.4.2 Use of Data

The Company uses your personal data to:

- Process and fulfil orders and keep you informed about the status of your or your company's order;
- Provide and administer our products and services;
- Provide customer support and process, evaluate, and respond to requests and inquiries;
- Conduct and facilitate customer satisfaction surveys;
- Conduct marketing and sales activities (including generating leads, pursuing marketing prospects, performing market research, determining, and managing the effectiveness of our advertising and marketing campaigns and managing our brand);
- Send you marketing communications (such as alerts, promotional materials, newsletters, etc.);
- Perform data analytics (e.g., market research, trend/financial analysis, and customer segmentation).

The Company only collects the personal data from you that it needs for the above purposes. The Company may also anonymize your personal data, so it no longer identifies you and use it for various purposes, including the improvement of our services and testing our IT systems.

5.4.3 When an Information Request is Refused by the Data Subject

Certain personal data is necessary to establish, conduct or terminate a business relationship with you. The Company need you to provide us with the personal data required for the fulfilment of contractual obligations or which the Company are legally obliged to collect. Without such personal data, the Company will not be able to establish, execute or terminate a contract with you. Also, the Company will be unable to take requested pre-contractual measures to enter a contract with you or to establish and continue the business relationship you have asked for.

5.4.4 Legal Basis

The Company uses your personal data for the purposes described in this notice based on one of the following legal bases, as applicable:

- The Company may process your personal data for the fulfilment of contractual obligations resulting from contracts with you or your company, or as part of pre-contractual measures the Company have been asked to take;
- The Company may process your personal data based on statutory requirements, for example, based on tax or reporting obligations, cooperation obligations with authorities or statutory retention periods;

- The Company will ask your consent for the activities described in this privacy notice when required by applicable law, for example when the Company processes your data for marketing purposes where the Company does not have an existing business relationship with you or your company; or
- The Company will rely on our legitimate interests to process your personal data within the scope of the business relationship with you or your company. Our legitimate interests to collects and uses the personal data for this purpose are management and furtherance of our business.

You may obtain a copy of our assessment of why the Company may process your personal data for these interests by submitting a request to the Company Contact identified in section 1.5.3 of this Policy.

5.5 Other Data Subject Types

5.5.1 Unsolicited Personal Information

If you send the Company unsolicited personal information, for example a CV, the Company reserves the right to immediately delete that information without informing you or to decide which category of data subject that you appear to be and manage your personal data within the remit of that category as described elsewhere in this Privacy Notice.

5.5.2 Website Users

The Company collects the following categories of personal data:

- The business contact information you share with us: name, title, job title, email address, business address, telephone number, mobile telephone number, etc.
- Information your browser makes available when you visit the Company website: IP address, the source of your site visit, time spent on the website or a particular page, links clicked, comments shared, browser type, date, and time of visit, etc.

5.5.3 Use of Data

The Company uses your personal data to:

- Respond to your specific request that you make, for example request a demonstration, whitepapers, newsletters, or other information.
- Provide customer support and process, evaluate, and respond to requests and inquiries;
- Conduct and facilitate customer satisfaction surveys;
- Conduct marketing and sales activities (including generating leads, pursuing marketing prospects, performing market research, determining, and managing the effectiveness of our advertising and marketing campaigns and managing our brand);
- Send you marketing communications (e.g., alerts, promotional materials, newsletters, etc.);
- Perform data analytics (such as market research, trend analysis, financial analysis, and customer segmentation).

The Company only collects the personal data from you that it needs for the above purposes. The Company may also anonymize your personal data, so it no longer identifies you and use it for various purposes, including the improvement of our services and testing our IT systems.

5.5.4 Legal Basis

The Company uses your personal data for the purposes described in this notice based on one of the following legal bases, as applicable:

- Legitimate interest as by using our website it is understood that there is potential for you to be a potential customer, contractor, employee, or supplier.

APPENDICES

Appendix A: References and Resources

ACTIVE AND EMERGING HEALTH PRIVACY LAWS AND REGULATIONS		
Name	**Link**	**Effective Date**
45 CFR Part 160	Title 45, Subtitle A, Subchapter C, Part 160	December 13, 2024
Subparts A and E of Part 164	Part 164—Security And Privacy	December 13, 2024
Combined Regulation Text of All Rules	45 CFR Part 160, Part 162, and Part 164	December 13, 2024
HIPAA Privacy Rule to Support Reproductive Health Care Privacy	45 CFR Parts 160 and 164 RIN 0945-AA20	December 23, 2024

Table 1: Active and Emerging Health Privacy Laws, and Regulations

ACTIVE AND EMERGING DATA PRIVACY LAWS AND REGULATIONS		
Name	**Link**	**Effective Date**
General Data Protection Regulation	GDPR	May 25, 2018
EU-U.S. Data Privacy Framework (EU-U.S. DPF) and, as applicable the UK Extension to the EU-U.S. DPF	DPF	July 10, 2023
California Consumer Privacy Act	CCPA	Jan. 1, 2020
California Privacy Rights Act	Proposition 24	Jan. 1, 2023
Colorado Privacy Act	SB 190	July 1, 2023
Connecticut Data Privacy Act	SB 6	July 1, 2023
Delaware Personal Data Privacy Act	HB 154	January 01, 2025
Indiana Consumer Data Protection Act	SB 5	January 01, 2026
Iowa Consumer Data Protection Act	SF 262	January 01, 2025
Kentucky Consumer Data Protection Act	HB 15	January 01, 2026
Maryland Online Data Privacy Act	SB 541	October 01, 2025

ACTIVE AND EMERGING DATA PRIVACY LAWS AND REGULATIONS		
Minnesota Consumer Data Privacy Act	HF 4757	July 31, 2025
Montana Consumer Data Privacy Act	SB 384	October 01, 2024
Nebraska Data Privacy Act	LB 1074	January 01, 2025
New Hampshire	SB 255	January 01, 2025
New Jersey	SB 332	January 15, 2025
Oregon Consumer Privacy Act	SB 619	July 01, 2024
Rhode Island Data Transparency and Privacy Protection Act	H 7787	January 01, 2026
Tennessee Information Protection Act	HB 1181	July 01, 2025
Texas Data Privacy and Security Act	HB 4	July 01, 2024
Utah Consumer Privacy Act	SB 227	Dec. 31, 2023
Virginia Consumer Data Protection Act	SB 1392	Jan. 1, 2023
ACTIVE BILLS		
Name	**Link**	
• Massachusetts Data Privacy Act • Massachusetts Data Privacy Protection Act (C) • Massachusetts Information Privacy and Security Act (C) • Internet Bill of Rights	• S 2770 ("In Committee") • H 83 ("In Committee") S 25 ("In Committee") • H 60 ("In Committee") S 227 ("In Committee") • HD3245 ("In Committee")	
Michigan Personal Data Privacy Act	SB 659 ("In Committee")	
Ohio Personal Privacy Act	HB 345 ("In Committee")	
• Pennsylvania Consumer Data Privacy Act • Pennsylvania Consumer Data Privacy Act (C)	• HB 1947 ("In Committee") • SB 1279 ("In Committee") HB 1201 ("In Cross Committee")	

Table 2: Active and Emerging Laws, Regulations, and Bills

Appendix B: Record Retention Schedule

The Retention Schedule lists categories of Records with the amount of time that each Record must be retained.

Record Type	Retention Period
Accounting and Financial	
Accounts Payable (Vendors)	7 years
Accounts Receivable (Customers)	7 years
Annual Audited Financial Statements and Audit Reports	Permanent
Annual Audit Records, including work papers	7 years after completion of audit
Annual Plans and Budgets	2 years
General Ledger and Trial Balance (year-end)	Permanent
Bank Statements, Reconciliations, Canceled Checks & Deposits	7 years
Customer Payment Records	7 years
Employee Expense Reports & support	7 years
Payroll Deduction, Contribution, Garnishment Authorizations	Termination + 7 years
Payroll Registers, Master Controls, Payroll supporting reports	7 years
Time Cards/Sheets (supersedes electronic media policy)	7 years
Quarterly and Annual Payroll Tax Reports	7 years
Vendor Records (W-2 and W-4 Forms)	7 years
401(k) Profit Sharing and Contribution Records	7 years
Licenses and Permits	5 years
Contracts, Legal Files, and Patents	
Contracts without contractual retention and/or contractual disposal requirement(s). and contract-related correspondence, including related proposals, drafts statement or work, quotes, etc.	7 years after contractual expiration the contract terminates or expires.
Legal Memoranda and Opinions	7 years after the matters is closed.
Litigation Files	3 years after expiration of appeals
Court Orders	Permanent
Patents	Permanent
Application for Patents	Permanent
Contract-Bound Records	
Ready Computing enters contracts with clients, suppliers, vendors, and other external parties. These contracts often, if not always, have specific	Per specific contract.

Record Type	Retention Period
explicit data retention and/or deletion/disposal clauses, provisions, and/or other such legalities by which the Company agrees to be bound by. Per specific contract.	
Employment Records	
Employee Personnel Records	Termination + 7 years
Employee Contracts	Termination + 7 years
Commissions, Bonuses, Incentives, & Awards	7 years
Employee Applications	1 year
Job Descriptions	Permanent
I-9's	Term + 1 yr. or Hire + 3 years, whichever is later
Insurance Records	
Annual Loss Summaries	Ten years
Audits and Adjustments	Three (3) years after final adjustment
Certificates	Permanent
Claims, including correspondence, medical records, injury, documents, etc.	Permanent
Group Insurance Plans	Until Plan is amended or terminated
Insurance Policies	Permanent
Release and Settlements	Permanent
Miscellaneous Records	
Internal Policy, Procedure, Plans, and other internal documentation.	Permanent
Property Records	
Original purchase, sales, lease agreements	Permanent
Property deeds, assessments, licenses, rights of way	Permanent
Property insurance policies	Permanent
Sales and Marketing Records	
All information collected on individuals via Company sales and marketing processes using emails, websites, and other marketing activities.	This information is retained until one of the following events prompts action: A Data Subject makes a formal Data Subject Request. A Data Subject uses the opt-out/unsubscribe function. The Company has reviewed the information on an annual basis and determined that we no longer have a legitimate need for retaining the information.

Record Type	Retention Period
Tax Records	
Annual information returns – Federal and State	Permanent
Excise Tax Records	Seven (7) years
IRS Rulings	Permanent
Sales use tax records	Seven (7) years
Tax Exemption Documents	Permanent
Tax Returns- Income, Franchise, and Property	Permanent
Tax work papers supporting tax returns	Permanent
Quarterly and Annual payroll tax records	Seven (7) years

Table 3: Retention Schedule Table

Appendix C: Compliance with the DPF and its Principles

The following information was created by The International Trade Administration (ITA), U.S. Department of Commerce and can be found by navigating to the following website. Additionally, though, and for clarity, all DPF Principles have also been included below for convenience.

Compliance Statement

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. Ready Computing has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) regarding the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

DPF Principles

The applicable DPF Principles that Ready Computing complies with are as follows:

1. Notice
2. Choice
3. Accountability for Onward Transfer
4. Security
5. Data Integrity and Purpose Limitation
6. Access
7. Recourse, Enforcement, and Liability

Key Requirements for DPF Program Participating Organizations

To clearly communicate the importance of the DPF and how the Company takes steps in adhering to the DPF Principles, it has made the following statements below:

Informing Individuals About Data Processing

- Ready Computing declares its commitment to comply with the DPF Principles.
- Ready Computing includes a link to the U.S. Department of Commerce's DPF program website and a link to or the web address for the relevant website or complaint submission form of the independent recourse mechanisms that is available to investigate individual complaints brought under the DPF Principles in 1. Introduction.
- Ready Computing informs individuals of their rights to access their personal data, the requirement to disclose personal information in response to lawful request by public authorities, which enforcement authority has jurisdiction over the participating organization's compliance with the DPF Principles, and the participating organization's liability in cases of onward transfer of data to third parties throughout this document.

Providing Free and Accessible Dispute Resolution

- Individuals may bring a complaint directly to Ready Computing, and Ready Computing will respond to the individual within 30 days.
- Ready Computing will provide, at no cost to the individual, an independent recourse mechanism by which each individual's complaints and disputes can be investigated and expeditiously resolved.
- If an individual submits a complaint to a data protection authority (DPA) in the European Union / European Economic Area, the United Kingdom (and/or, as applicable, Gibraltar), the U.S. Department of Commerce's International Trade Administration (ITA) has committed to receive, review, and undertake best efforts to facilitate resolution of the complaint and to respond to the DPA within 90 days.
- Ready Computing commits to binding arbitration at the request of the individual to address any complaint that has not been resolved by other recourse and enforcement mechanisms. Please refer to Annex I for more information.

Cooperating with the U.S. Department of Commerce

- Ready Computing will respond promptly to inquiries and requests by the ITA for information relating to the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and, as applicable the UK Extension to the EU-U.S. DPF.

Maintaining Data Integrity and Purpose Limitation

- Ready Computing will limit personal information to the information relevant for the purposes of processing.
- Ready Computing will comply with the data retention provision.

Ensuring Accountability for Data Transferred to Third Parties

To transfer personal information to a third party acting as a controller, Ready Computing will:

- Comply with the Notice and Choice Principles; and
- Enter a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the DPF Principles and will notify the organization if it determines that it can no longer meet this obligation. The contract shall provide that when a determination is made the third-party controller ceases processing or takes other reasonable and appropriate steps to remediate.

To transfer personal data to a third party acting as an agent, Ready Computing will:

- Transfer such data only for limited and specified purposes;
- Ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the DPF Principles;
- Take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the DPF Principles;
- Require the agent to notify the organization if it decides that it can no longer meet its obligation to provide the same level of protection required by the DPF Principles;
- Upon notice, take reasonable and appropriate steps to stop and remediate unauthorized processing; and
- Provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the U.S. Department of Commerce upon request.

Ensuring Commitments Are Kept as Long as Data Is Held

- If Ready Computing leaves the relevant part(s) of the DPF program, it will annually affirm to the ITA its commitment to apply the DPF Principles to information received under the relevant part(s) of the DPF program if it chooses to keep such data; otherwise, it will provide "adequate" protection for the information by another authorized means.

Appendix D: Revision History

Revision history is maintained and can be requested.