RIA™ Data Processing Addendum

(Annotated Draft for Legal Review)

Effective Date: _March 26, 2026_____

This Data Processing Addendum ("DPA") forms part of the RIA™ Terms of Use and governs the processing of Personal Data by Climate Resilience Consulting LLC ("CRC," "we," "our," or "us") on behalf of government or organizational subscribers ("Customer") using the Resilience Intelligence Advantage platform ("RIA" or the "Platform").

This DPA applies whenever CRC processes Personal Data on behalf of a Customer in connection with the RIA platform.

1. Definitions

For purposes of this DPA:

Personal Data means any information relating to an identified or identifiable individual that is processed by CRC on behalf of the Customer through the RIA platform.

Processing means any operation performed on Personal Data, including collection, storage, use, transmission, disclosure, or deletion.

Controller means the entity that determines the purposes and means of processing Personal Data.

Processor means the entity that processes Personal Data on behalf of the Controller.

Subprocessor means a third party engaged by CRC to assist in processing Personal Data in connection with the RIA platform.

Customer acts as the **Controller** of Personal Data submitted to the platform. CRC acts as a **Processor** and processes Personal Data only as described in this DPA and the RIA Terms of Use.

2. Scope of Processing

CRC processes Personal Data solely for the purpose of providing and supporting the RIA platform and related services.

Such processing may include:

- authenticating authorized Users
- enabling access to the platform
- maintaining platform security
- providing customer support
- monitoring system performance
- maintaining system logs necessary for security and troubleshooting

The categories of Personal Data processed may include user names, email addresses, organizational roles, login timestamps, activity logs, and support communications. System logs and technical metadata may contain identifiers necessary for platform security and troubleshooting.

RIA is designed to minimize the collection of Personal Data and does not intentionally collect sensitive personal information such as financial data, health information, or government identification numbers.

3. Processing Instructions

CRC processes Personal Data only on documented instructions from the Customer, except where processing is required by applicable law.

Customer instructs CRC to process Personal Data as necessary to provide the RIA platform and related support services in accordance with the Terms of Use and this DPA.

CRC does not sell Personal Data, use Personal Data for advertising purposes, or use Personal Data to train artificial intelligence or machine-learning models.

CRC may use anonymized or aggregated information derived from platform activity for the limited purpose of monitoring system performance and improving platform functionality, provided such information does not identify individuals or Customer organizations.

4. Subprocessors

CRC may engage Subprocessors to support operation of the RIA platform, including secure hosting providers, infrastructure services, cybersecurity monitoring services, and other technical service providers.

CRC requires all Subprocessors to process Personal Data only as necessary to support the platform and to maintain confidentiality and appropriate security safeguards.

CRC maintains oversight of Subprocessors and remains responsible for their compliance with applicable data protection obligations under this DPA.

Upon reasonable request, CRC will provide Customers with information regarding Subprocessors used to support the RIA platform. CRC will notify Customers of material changes to Subprocessors where required by applicable law or contractual obligation.

5. Security Measures

CRC implements administrative, technical, and organizational safeguards designed to protect Personal Data from unauthorized access, disclosure, alteration, or destruction.

These safeguards include secure cloud infrastructure, encrypted data transmission, role-based access controls, identity and password management systems, system monitoring and logging, incident response procedures, and security training for personnel.

Access to Personal Data is limited to authorized CRC personnel who require such access to perform their job responsibilities. All access to Personal Data is subject to monitoring and internal access controls.

CRC may provide Customers with reasonable information regarding its security practices or documentation sufficient to demonstrate compliance with this DPA upon request.

6. Assistance with Data Subject Rights

To the extent required by applicable law, CRC will provide reasonable assistance to Customers in responding to requests from individuals seeking to exercise their privacy rights, including requests for access, correction, or deletion of Personal Data.

Customer remains responsible for responding to such requests and determining whether such requests should be granted under applicable law.

7. Data Retention and Deletion

CRC retains Personal Data only for the period necessary to provide the platform services, maintain system security, comply with legal obligations, and support legitimate operational needs.

Upon termination of the Customer’s subscription or upon written request from the Customer, CRC will delete or return Personal Data within a reasonable period unless retention is required by law or necessary for system integrity.

CRC may retain anonymized or aggregated information derived from platform activity provided such information cannot reasonably identify individuals or Customer organizations.

CRC requires Subprocessors to comply with equivalent deletion and retention obligations when processing Personal Data on CRC's behalf.

8. Data Breach Notification

CRC maintains procedures to detect, investigate, and respond to potential security incidents affecting Personal Data.

If CRC becomes aware of a confirmed breach of Personal Data affecting Customer Data, CRC will notify the Customer without unreasonable delay.

Such notification will include available information regarding the nature of the incident, the categories of affected data, and steps taken or proposed to mitigate the incident where such information is available.

9. Customer Responsibilities

Customer represents and warrants that it has the legal authority to provide Personal Data to CRC for processing through the RIA platform.

Customer is responsible for ensuring that Personal Data uploaded to the platform is collected and processed in accordance with applicable privacy laws.

Customer is also responsible for managing user access permissions and ensuring that authorized Users comply with the Customer's internal data protection policies.

Customer agrees not to upload highly sensitive personal information to the platform unless explicitly authorized by CRC in writing.

10. Governing Law

This DPA is governed by the law specified in the RIA Terms of Use or applicable subscription agreement between CRC and the Customer.

Any disputes arising under this DPA will be resolved in accordance with the dispute resolution provisions contained in the RIA Terms of Use.

11. Relationship to Other Agreements

This DPA supplements and forms part of the RIA Terms of Use governing the Customer's access to the platform.

In the event of a conflict between this DPA and the Terms of Use with respect to the processing of Personal Data, the provisions of this DPA will govern.