RAINFOCUS DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is incorporated into and forms part of the Master Subscription and Services Agreement (the "Agreement") between RainFocus, LLC ("Processor" or "RainFocus") and the entity identified in the applicable Order Form ("Controller" or "Client"). This DPA governs the processing of Personal Data by Processor on behalf of Controller in connection with the Services.

1. DEFINITIONS

"Data Privacy Laws" means all applicable laws relating to data protection and privacy, including the GDPR, UK GDPR, and U.S. state privacy laws (including CCPA/CPRA, Virginia CDPA, Colorado CPA, Connecticut CTDPA, and Utah UCPA), as amended from time to time.

"Data Subject" means an identified or identifiable natural person whose Personal Data is processed.

"Personal Data" means any information relating to a Data Subject that is protected under applicable Data Privacy Laws.

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

"Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

"Subprocessor" means any third party engaged by Processor to process Personal Data on behalf of Controller.

2. ROLES AND SCOPE

2.1 Roles. Controller determines the purposes and means of processing Personal Data. Processor processes Personal Data solely on behalf of Controller in accordance with this DPA and Controller's documented instructions.

2.2 Scope. Processor will process the categories of Personal Data and Data Subjects described in Schedule 1, for the purposes of providing the Services under the Agreement.

3. PROCESSOR OBLIGATIONS

3.1 Processing Instructions. Processor shall process Personal Data only in accordance with Controller's documented instructions, except where required by applicable law. The Agreement and this DPA constitute Controller's complete instructions. Processor shall promptly inform Controller if an instruction appears to violate Data Privacy Laws.

3.2 Compliance. Processor warrants that its processing activities will comply with applicable Data Privacy Laws.

3.3 Confidentiality. Processor shall ensure that personnel authorized to process Personal Data are subject to confidentiality obligations and receive appropriate training.

3.4 Limitations on Use. Processor shall not: (a) sell or share Personal Data; (b) retain, use, or disclose Personal Data for any purpose other than providing the Services; or (c) combine Personal Data with data from other sources, except as permitted by applicable law.

4. SECURITY

4.1 Security Measures. Processor shall implement and maintain appropriate technical and organizational security measures to protect Personal Data, as described in Schedule 2. These measures include encryption of data in transit and at rest, access controls, and regular security assessments.

4.2 Security Assessments. Processor shall conduct documented security assessments at least annually.

5. SECURITY INCIDENTS

5.1 Notification. Processor shall notify Controller of a Security Incident without undue delay, and in any event within seventy-two (72) hours after confirmation. Notification shall include, to the extent known: (a) the nature of the incident; (b) categories and approximate number of affected Data Subjects; (c) likely consequences; and (d) measures taken or proposed to address the incident.

5.2 Cooperation. Processor shall provide reasonable cooperation to assist Controller in meeting its breach notification obligations under Data Privacy Laws.

6. SUBPROCESSORS

6.1 Authorization. Controller authorizes Processor to engage Subprocessors to process Personal Data. The current list of Subprocessors is available at https://www.rainfocus.com/privacy-security/subprocessors/.

6.2 Notice of Changes. Processor will provide Controller at least fourteen (14) days' prior written notice before engaging a new Subprocessor or making material changes to existing Subprocessor arrangements.

6.3 Objections. Controller may object to a new Subprocessor within thirty (30) days of notice by providing written notice with documented, reasonable grounds related to data protection. The Parties will discuss the objection in good faith. If no resolution is reached within fifteen (15) days, Controller's sole remedy is to terminate the affected Services upon thirty (30) days' notice.

6.4 Subprocessor Obligations. Each Subprocessor will be bound by data protection obligations substantially similar to those in this DPA.

6.5 Liability. Processor remains liable for its Subprocessors' compliance with this DPA.

7. DATA SUBJECT RIGHTS

Processor shall promptly notify Controller of any Data Subject request and provide reasonable assistance in responding to such requests, taking into account the nature of the processing.

8. CONTROLLER OBLIGATIONS

8.1 Lawful Basis. Controller is responsible for: (a) ensuring a lawful basis for processing; (b) providing required notices to Data Subjects; (c) obtaining necessary consents; and (d) the accuracy and legality of Personal Data provided to Processor.

8.2 Instructions. Controller shall ensure its processing instructions comply with applicable law.

9. INTERNATIONAL TRANSFERS

9.1 Transfer Mechanisms. Transfers of Personal Data from the EEA, UK, or Switzerland to countries without an adequacy determination shall be governed by: (a) the EU Standard Contractual Clauses (Module 2 or 3, as applicable); (b) the UK International Data Transfer Addendum; (c) the EU-U.S. Data Privacy Framework (where Processor maintains valid certification); or (d) another valid transfer mechanism under applicable law.

9.2 SCCs. Where Standard Contractual Clauses apply, the Schedules to this DPA shall populate the required annexes. Execution of this DPA constitutes execution of the SCCs.

10. AUDITS

10.1 Audit Rights. Upon Controller's reasonable written request (no more than once annually), Processor shall provide information necessary to demonstrate compliance with this DPA. Processor may satisfy audit requests by providing its current SOC 2 Type II report, ISO 27001 certification, or equivalent third-party audit report.

10.2 On-Site Audits. If Controller reasonably determines third-party reports are insufficient, Controller may request an on-site audit with at least thirty (30) days' notice, during business hours, limited to systems processing Controller's Personal Data. Controller bears its own costs and shall reimburse Processor's reasonable costs for on-site audits beyond the provision of reports.

11. DATA RETENTION AND DELETION

Upon termination of the Agreement or Controller's earlier written request, Processor shall delete or return Personal Data within ninety (90) days, except where retention is: (a) required by law; (b) contained in backup systems maintained in accordance with standard retention policies; or (c) necessary for Processor's legitimate compliance or legal purposes. Retained data remains subject to this DPA.

12. LIABILITY

Liability arising under this DPA is subject to the limitations of liability in the Agreement.

13. U.S. STATE PRIVACY LAWS

To the extent Processor processes Personal Data subject to U.S. state privacy laws, Processor acts as a "Service Provider" or "Processor" under such laws and certifies it understands and will comply with applicable restrictions, including restrictions on selling, sharing, and using Personal Data outside the direct business relationship.

14. GENERAL

14.1 Conflict. In the event of conflict between this DPA and the Agreement, this DPA governs with respect to Personal Data processing.

14.2 Duration. This DPA remains in effect for the duration of Processor's processing of Personal Data under the Agreement.

SCHEDULE 1: PROCESSING DETAILS

Element	**Description**
Data Subjects	Event attendees and users of the Services
Categories of Personal Data	Name, email address, IP address, and other registration data as configured by Controller
Processing Activities	Collection, storage, organization, retrieval, use, and deletion as necessary to provide the Services
Purpose	Provision of event management and registration services under the Agreement
Duration	For the Term of the Agreement

SCHEDULE 2: SECURITY MEASURES

Processor implements and maintains the following security measures:

1. Access controls restricting Personal Data access to authorized personnel based on business need
2. Unique authentication for all users with access to Personal Data
3. Encryption of Personal Data in transit and at rest using industry-standard protocols
4. Physical security controls for facilities housing systems that process Personal Data
5. Network segregation between internal systems and public networks
6. Anti-malware protection on systems processing Personal Data
7. Monitoring and alerting capabilities
8. Vulnerability management and timely deployment of security updates
9. Annual penetration testing by qualified third parties
10. Security and privacy training for personnel
11. Redundancy and backup procedures for data availability
12. Documented incident response procedures
13. Security evaluation of Subprocessors