

Data Processing Agreement

This Data Processing Addendum (“**DPA**”) is entered into by and between **Automatic Capital Operations Pty Ltd**, a company incorporated in Australia with its principal place of business at 17 Henry Street, Spring Hill, QLD, 4000, Australia (“**AutoRFP**”), and the customer entity identified on the applicable Order Form (“**Customer**”).

This DPA governs the Processing of Personal Data by AutoRFP on Customer’s behalf in connection with its provision of the Platform and is incorporated into and forms part of the Master Services Agreement or other written agreement between the parties (the “**Main Agreement**”).

Capitalized terms used but not defined in this SLA will have the meaning given to them in the MSA.

1. Definitions.

- 1.1. “**Customer Data**” means any and all data, content, and information, including Personal Data, submitted by or on behalf of Customer or its authorized users to the Platform, or generated by the Platform for the Customer in the course of providing the Services.
- 1.2. “**Data Protection Laws**” means all applicable laws, regulations, and other legal requirements relating to privacy, data security, and the processing of Personal Data, including but not limited to the GDPR, UK GDPR, PIPEDA, the Australian *Privacy Act 1988* (Cth), and US Privacy Laws.
- 1.3. “**Data Subject**” means the identified or identifiable natural person to whom Personal Data relates.
- 1.4. “**GDPR**” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
- 1.5. “**Personal Data**” means any information relating to a Data Subject that is part of the Customer Data Processed by AutoRFP on behalf of Customer in connection with the Main Agreement.
- 1.6. “**Platform**” means the AutoRFP software-as-a-service platform and related services contracted by Customer under the Main Agreement.

Data Processing Agreement

- 1.7. "Process", "Processes", or "Processing"** means any operation or set of operations which is performed on Personal Data, whether or not by automated means.
- 1.8. "Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by AutoRFP.
- 1.9. "Standard Contractual Clauses" or "SCCs"** means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679.
- 1.10. "Sub-processor"** means any third party engaged by AutoRFP to Process Personal Data in connection with the Platform.
- 1.11. "UK GDPR"** means the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
- 1.12. "US Privacy Laws"** means, as applicable, US state privacy laws including the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA").

2. Processing of Personal Data

- 2.1. Roles and Responsibilities.** The parties acknowledge that for the purposes of Data Protection Laws, Customer is the data controller (or a processor acting on behalf of a controller) and AutoRFP is the data processor. AutoRFP will Process Personal Data only in accordance with Customer's documented lawful instructions, including as set forth in this DPA and the Main Agreement. The details of the Processing are described in **Schedule 1**.
- 2.2. Prohibition on AI Model Training.** Notwithstanding any other provision of the Main Agreement or this DPA, AutoRFP shall not, under any circumstances, use Customer Data to train, fine-tune, or otherwise improve any artificial intelligence models, machine learning systems, or any other algorithms for its own purposes or for the benefit of any third party. Notwithstanding the

Data Processing Agreement

foregoing, Customer Data may be used to train Customer tenant-specific AI models to provide customized findings and recommendations to Customer solely for Customer's benefit. Customer Data shall be used solely for the purpose of providing the Platform and its functionalities to Customer.

- 2.3. Compliance with Laws.** AutoRFP will promptly inform Customer if, in its opinion, an instruction from Customer infringes applicable Data Protection Laws, unless prohibited from doing so by law.

3. Security

- 3.1. Security Measures.** Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, AutoRFP shall implement and maintain appropriate technical and organizational security measures designed to protect Personal Data against a Security Incident and to ensure a level of security appropriate to the risk. These measures are detailed in **the Security Exhibit** attached by reference hereto ("**Security Measures**"). AutoRFP shall not materially decrease the overall security of the Platform during the term of the Main Agreement.
- 3.2. Confidentiality.** AutoRFP shall ensure that its personnel authorized to Process Personal Data are subject to binding obligations of confidentiality.

4. Security Incident Notification

- 4.1. Notification.** Upon becoming aware of a Security Incident, AutoRFP will notify Customer without undue delay, and in any event within forty-eight (48) hours.
- 4.2. Cooperation.** AutoRFP will provide Customer with timely information about the Security Incident, including the nature of the incident, the data affected, and the remedial actions being taken, as it becomes known or as is reasonably requested by Customer. AutoRFP will provide reasonable cooperation to Customer in its investigation and mitigation of the Security Incident.

Data Processing Agreement

5. Sub-processing.

- 5.1. Authorization.** Customer provides a general authorization for AutoRFP to engage Sub-processors to provide the Platform. The current list of Sub-processors is available at <https://autorfp.ai/trust/subprocessors>.
- 5.2. Obligations.** AutoRFP will enter into a written agreement with each Sub-processor imposing data protection obligations that are at least as protective as those in this DPA. AutoRFP shall remain liable for the acts and omissions of its Sub-processors to the same extent AutoRFP would be liable if it were performing the services of each Sub-processor directly under the terms of this DPA.
- 5.3. Changes.** AutoRFP will provide Customer with at least fourteen (14) days' prior written notice of any new Sub-processor. Customer may object to the appointment in writing within seven (7) days of such notice on reasonable data protection grounds. If the parties are unable to resolve the objection in good faith, either party may terminate the Main Agreement for convenience.

6. Data Subject Rights

- 6.1. Assistance Provided.** Taking into account the nature of the Processing, AutoRFP will provide reasonable assistance to Customer, through appropriate technical and organizational measures, to enable Customer to respond to requests from Data Subjects exercising their rights under Data Protection Laws.

7. Audits

- 7.1. Audit Reports Available.** AutoRFP shall make available to Customer all information reasonably necessary to demonstrate compliance with this DPA, including its most recent third-party audit reports.
- 7.2. Audit Rights.** To the extent such reports are not sufficient to demonstrate compliance, Customer (or a qualified, independent third-party auditor, subject to reasonable confidentiality obligations) may conduct an audit of AutoRFP's compliance with this DPA, at Customer's expense, no more than once annually, upon 30 days' prior written notice, and during normal business hours, in a manner designed to minimize disruption to AutoRFP's business.

Data Processing Agreement

8. Return and Deletion of Data

- 8.1.** Upon termination of the Main Agreement, AutoRFP shall, at Customer's election, either return or securely delete all Customer Data in its possession, unless applicable law requires retention.

9. Cross-Border Data Transfers & Jurisdictional Terms

- 9.1. Transfers.** Personal Data may be transferred to and Processed in Canada, Australia, the United States, and other locations where AutoRFP or its Sub-processors maintain operations. AutoRFP will ensure such transfers comply with applicable Data Protection Laws.
- 9.2. Jurisdictional Requirements.** The jurisdiction-specific terms in **Schedule 2** shall apply to the Processing of Personal Data as specified therein.

10. General Provisions

- 10.1. Liability.** The total aggregate liability of either party arising out of or related to this DPA shall be subject to the limitations of liability set forth in the Main Agreement.
- 10.2. Conflict.** In the event of any conflict between this DPA and the Main Agreement, the terms of this DPA shall prevail with respect to the subject matter of data protection.
- 10.3. Governing Law.** This DPA shall be governed by and construed in accordance with the governing law specified in the Main Agreement.

Data Processing Agreement

SCHEDULE 1: DETAILS OF PROCESSING

Item	Description
Data Subjects	Customer's employees, contractors, business partners, and other individuals whose Personal Data is included in the Customer Data submitted to the Platform by Customer.
Categories of Personal Data	Categories of Personal Data are determined and controlled by Customer, but may include business contact information (name, title, email, phone number), professional details, and any other Personal Data contained within RFP questions, security questionnaires, and other documents uploaded to the Platform.
Special Categories of Data	None intended. Customer agrees not to upload any sensitive or special categories of personal data (e.g., health, financial, or government-issued ID numbers) to the Platform unless expressly agreed in writing with AutoRFP.
Nature and Purpose of Processing	To provide the AutoRFP Platform and related services to Customer as described in the Main Agreement. The core processing activity involves ingesting and analyzing Customer Data to automatically generate draft responses to RFPs, RFIs, and security questionnaires, and to manage a library of approved content for such responses, all as directed by the Customer.
Duration of Processing	For the term of the Main Agreement, plus any period required for data deletion/return as outlined in this DPA.

Data Processing Agreement

SCHEDULE 2: JURISDICTION-SPECIFIC TERMS

Part A: European Economic Area (EEA), United Kingdom (UK) & Switzerland

(1) Data Transfer Mechanism

(a) Primary Basis for Transfer: The parties acknowledge that AutoRFP Processes Personal Data in Canada, a country recognized by the European Commission and the United Kingdom as providing an adequate level of data protection for commercial organizations. Accordingly, transfers of Personal Data from the EEA, UK, and Switzerland to AutoRFP in Canada are made on the basis of these adequacy decisions.

(b) Alternative Transfer Mechanism: To the extent that Personal Data is transferred to, or accessed by, AutoRFP or its Sub-processors in a country that is not subject to an adequacy decision (a **"Third Country"**), such transfers shall be governed by the appropriate data transfer agreements as follows:

- (i) For the European Economic Area (EEA):** The Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, as approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the **"EU SCCs"**), Module Two (Controller to Processor), are incorporated by reference.
- (ii) For the United Kingdom (UK):** The International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner's Office, version B1.0 (the **"UK Addendum"**), is incorporated by reference.
- (iii) For Switzerland:** For transfers subject to the Swiss Federal Act on Data Protection (**"FADP"**), the EU SCCs will apply, modified as necessary to comply with the FADP, including referencing the FADP and the Swiss Federal Data Protection and Information Commissioner as the competent supervisory authority.

(2) Details for the SCCs and UK Addendum For the purposes of the EU SCCs and the UK Addendum:

Data Processing Agreement

- (a) The information set forth in **Schedule 1 (Details of Processing)** of this DPA shall be deemed to complete Annex I of the EU SCCs and Part 1 of the UK Addendum.
- (b) The technical and organizational measures set forth in **the Security Exhibit (Security Measures)** incorporated by reference hereto to this DPA shall be deemed to complete Annex II of the EU SCCs.
- (c) For the optional clause 7 (Docking Clause) of the EU SCCs, the docking clause shall not apply.
- (d) For clause 17 (Governing Law) of the EU SCCs, the governing law shall be the law of Ireland. For clause 18 (Choice of forum and jurisdiction), the courts of Ireland shall have jurisdiction.

(3) Transfers to Sub-processors. AutoRFP will ensure that its transfers to any Sub-processors in the United States are subject to a valid transfer mechanism, which may include the EU-U.S. Data Privacy Framework, the UK Extension thereto, and the Swiss-U.S. Data Privacy Framework, or the execution of the appropriate SCCs.

Part B: United States

(1) Scope and Roles. This Part B applies to the Processing of Personal Data subject to US Privacy Laws, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (the **"CCPA"**). For the purposes of the CCPA, Customer is a "Business" and AutoRFP is a "Service Provider."

(2) Service Provider Obligations. AutoRFP certifies that it understands the restrictions and its obligations as a Service Provider under the CCPA and will comply with them. In its capacity as a Service Provider, AutoRFP shall:

- (a) Process Personal Data only for the limited and specified business purposes described in Schedule 1 of this DPA and in accordance with Customer's lawful instructions.
- (b) Not "Sell" or "Share" Personal Data (as such terms are defined in the CCPA).
- (c) Not retain, use, or disclose Personal Data for any commercial purpose other than the business purposes specified in the Main Agreement and this DPA, or as otherwise permitted by the CCPA.

Data Processing Agreement

- (d)** Not retain, use, or disclose Personal Data outside of the direct business relationship between the parties, unless expressly permitted by the CCPA.
- (e)** Not combine Personal Data which it receives from or on behalf of Customer with personal information that it receives from, or on behalf of, another person or collects from its own interaction with the Data Subject, except as permitted under the CCPA.
- (f)** Notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.
- (g)** Provide reasonable assistance to Customer in facilitating compliance with its obligations under US Privacy Laws, including with respect to responding to verifiable consumer requests to exercise their rights under the CCPA.