AutoRFP.ai Data Processing Agreement

Date	The date of the Order Form between the parties.
Company	The party identified as AutoRFP.ai in the Order Form.
Customer	The party identified as You in the Order Form.

The parties agree that this Data Processing Agreement (**DPA**) is incorporated into the Order Form executed by the parties.

Each Party agrees to comply with the provisions of this Data Processing Agreement (**DPA**), in exchange for the other Party also agreeing to be bound by this DPA.

EXECUTED as an AGREEMENT

SIGNED for and on behalf of Automatic Capital Operations Pty Ltd (ABN 24 666 447 230):	
Authorised Representative:	Signature:

SIGNED for and on behalf of (No.) in accordance with section 127 of the Corporations Act 2001 (Cth):	
Authorised Representative:	Signature:

1. Subject and application of the Agreement

1.1 This DPA (including Annexes I, II and III attached to it) applies only to the extent the Company receives Personal Data of Data Subjects who ordinarily reside in the United Kingdom or in a European Union member state from, or on behalf of, the Customer under the Head Agreement and the Company processes such Personal Data outside of the United Kingdom or European Economic Area. This DPA will not apply in any other circumstances.

1.2 To the extent this DPA applies, its provisions are incorporated into and form part of the Head Agreement.

2. Definitions

2.1 Unless otherwise defined herein, capitalized terms and expressions used in this DPA have the following meanings:

a. **"DPA"** means this data processing agreement;

b. **"Controller"** has the meaning given to that term (or an equivalent term) under the applicable Data Protection Law;

c. **"Customer Data"** means any Personal Data provided to the Customer by the Customer or on behalf of the Customer under or in connection with the Head Agreement;

d. **"Data Protection Laws"** means applicable laws and regulations in respect of the collection, use and handling of Personal Data, which includes (without limitation) the GDRP and Australia's *Privacy Act 1988* (Cth);

e. **"Data Subject"** means an identified or identifiable natural person, and includes any person defined as a Data Subject or a similar term under the applicable Data Protection Law;

f. **"GDPR"** means:

i. when used in the context of United Kingdom residents, means the UK General Data Protection Regulation as implemented by the *Data Protection Act 2018* (UK); and

ii. when used in the context of European Union residents, means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 for the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC;

g. **"Head Agreement"** means the contract between the Company and the Customer regarding the provision of the Company's software to the Customer;

h. **"Parties"** means the Company and the Customer;

i. **"Personal Data"** has the meaning given to the terms "personal data" or "personal information", or an equivalent term in the applicable Data Protection Law;

j. "**Personal Data Breach**" has the meaning given to that term (or an equivalent term) under the applicable Data Protection Law;

k. "**Processing**" and **"Process"** has the meaning given to that term (or an equivalent term) under the applicable Data Protection Law;

l. **"Processor"** has the meaning given to that term (or an equivalent term) under the applicable Data Protection Law;

m. **"Security Measures"** means the technical and organisational measures to protect the Customer Data from a Personal Data Breach, having regard to the state of the art, the costs of implementation and the nature of the Customer Data, the scope, context and purposes of Processing and, as appropriate, the Standard Contractual Clauses and the measures referred to in Article 32(1) of the GDPR.

n. "**Services**" means the Company's online platform for facilitating the vendor relationship management, electronic tendering / quoting and other related procurement activities and the associated services provided by the Company to the Customer under the Head Agreement;

o. **"Standard Contractual Clauses**" means:

i. in the context of United Kingdom residents, the standard contractual clauses between controllers and processors for compliance with the restricted transfer rules in the GDPR, as issued, amended or replaced in accordance with section 119A of the *Data Protection Act 2018* (UK);

ii. in the context of European Union residents, the standard contractual clauses set out in the Annex to Commission implementing decision (EU) 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 of the European Parliament and of the Council of 27 April 2016, including such clauses as amended or replaced from time to time; or

p. **"Subprocessor**" means any person appointed by or on behalf of the Company to process Personal Data in connection with the Head Agreement, including those specified in Annex III of this DPA; and

2.2 If a capitalised term is used but not defined in this DPA, the meaning given to that term under the Head Agreement will apply.

3. Scope of Processing

3.1 The Parties acknowledge and agree that:

a. the Customer remains the Controller of the Customer Data and will provide written instructions to the Company regarding the Processing of Customer Data; and

b. Company will act as a Processor of the Customer Data in accordance with the written instructions of the Customer.

3.2 The Company will comply with applicable Data Protection Laws in the Processing of Customer Data.

3.3 The Company will process the Customer Data in accordance with the instructions of the Customer unless the Company is legally required to do otherwise. If the Company determines (acting reasonably) that the Customer's instructions will or are likely to result in a breach of this DPA or applicable Data Protection Laws, the Company will inform the Customer of such risk, and the Parties acknowledge and agree that any failure by the Company to comply with such of the Customer's instructions will not constitute a breach of this DPA by the Company.

3.4 The Company will not:

a. other than in the performance or provision of the Services to Customer, sell or commercialise the Customer Data without first anonymising it in such a manner that the Customer cannot be identified and Personal Data can no longer be attributed to a specific Data Subject; or

b. use, hold or disclose the Customer Data for any purpose or in any manner other than as set out in the Head Agreement and this DPA.

3.5 The Company may process and use the Customer Data for the Company's own purposes as controller to the extent legally permitted by Data Protection Laws. This DPA does not apply to such data processing or use.

3.6 The Customer acknowledges and agrees that the Company is not responsible for:

a. ensuring the Customer's compliance with the applicable Data Protection Laws including in its capacity as the Controller towards Customer Data or other Personal Data; or

b. procuring any consent, authorisation or any agreement from the Customer's vendors to enable the Company to Process the Customer Data including as contemplated in the Head Agreement or this DPA.

3.7 The Parties agree that, to the extent that the Processing of Customer Data takes place outside the United Kingdom or European Economic Area (EEA) as applicable, the applicable Standard Contractual Clauses are incorporated into this DPA and apply to such Processing. The Parties agree that the Module specified in Annex I to this DPA is selected, or if no module is selected in Annex 1 then the selected Module is Module 2. All other Modules are deleted entirely.

4. Customer warranties

4.1 The Customer warrants that:

a. it has obtained all necessary consents and authorisations, or has otherwise established a legitimate legal basis to enable the Company to Process the Customer Data; and

b. any instructions provided to the Company in respect of Customer Data will not cause the Company to breach the applicable Data Protection Laws.

4.2 Should third parties assert claims against the Company based on the Processing of Customer Data in accordance with this DPA, the Customer will indemnify the Company from any costs, loss or damage arising from or in relation to such claims.

4.3 If the Company is required to provide information to a governmental body or person on the Processing of Customer Data or to cooperate with these bodies in any other way, the Customer is obliged to assist the Company in providing such information and in fulfilling other appropriate cooperation obligations.

5. Security of Processing

5.1 The Company will implement and maintain appropriate Security Measures to protect the Customer Data from a Personal Data Breach.

5.2 At the date of this DPA, the implemented Security Measures include the measures as listed in Annex II.

5.3 The Company may update and modify the Security Measures from time to time, provided such updates do not materially adversely affect the security of Customer Data and that the Company.

5.4 For clarity, the Company does not: share Personal Data with any third party not listed as a Subprocessor; or sell any Personal Data.

6. Engagement of Subprocessors

6.1 The Customer authorises the Company to engage and continue to engage Subprocessors with regard to the Processing of Customer Data. Subprocessors engaged as at the date of this DPA are listed in Annex III.

6.2 Without limiting clause 6.1, the Customer authorises the Company to appoint Subprocessors provided that:

a. the Company provides the Customer 30 days' prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor;

b. the Company provides the Customer written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor, and the Customer subsequently opts-in to the services provided by that Subprocessor;

c. each Subprocessor is subject to obligations no less onerous than those set out in this DPA in respect of Processing Customer Data; and

d. the Company agrees that it is responsible for all acts and omissions of its Subprocessors.

6.3 No authorization is required for contractual relationships with service providers that are concerned with the examination or maintenance of data processing procedures or systems by third parties or that involve other additional services, even if access to Customer Data cannot be excluded, as long as the Company takes reasonable steps to protect the confidentiality of the Customer Data.

6.4 In order to receive notifications with respect to adding or replacing existing Subprocessors, Customers may subscribe to a mailing list using the following link: autorfp.ai/trust/subprocessors.

6.5 The Customer may object to the appointment of a Subprocessor by giving written notice to the Company within 7 days of a notice of appointment of Subprocessor under this section 6, and the Customer's notice must particularise the Customer's reasonable grounds of objection. Upon the Company's receipt of the Customer's objection, the Parties will work together in good faith to resolve the Customer's concerns regarding the proposed Subprocessor. If the Parties are unable to resolve the Customer's concerns within 14 days , the Company may terminate the Head Agreement and this DPA immediately.

6.6 Subject to compliance with the requirements of section 3.7, the provisions of this section 6 will apply if a Subprocessor in a third country is involved.

7. Data Subjects' Rights

7.1 If the Company receives a request from a Data Subject to exercise their statutory rights under the applicable Data Protection Laws, the Company will:

a. promptly notify the Customer of such request and provide the Customer all information regarding the Data Subject's request; and

b. provide the Customer all reasonable assistance required by the Customer to respond to such Data Subject requests, including any requests for deletion of Personal Data.

7.2 The Customer acknowledges and agrees that, other than acknowledging receipt of the Data Subject's request (at the Company's sole discretion), the Company is not responsible for responding to or addressing requests from Data Subjects, and the Company will not do so in absence of Customer's instructions and (unless the Parties otherwise agree) at Customer's cost.

8. Personal Data Breach

8.1 If the Company becomes aware of an actual or suspected Personal Data Breach affecting Customer Data, the Company will:

a. promptly (and subject to the notice requirements under the applicable Data Protection Law) notify the Customer of such Personal Data Breach; and

b. provide the Customer any assistance reasonably required by the Customer to fulfill its obligations under Data Protection Laws applicable to the Personal Data Breach, including (without limitation) by providing the Customer any information regarding the Personal Data Breach.

8.2 Subject to clause 8.3, the Company will make reasonable efforts to conduct data protection impact assessments, and prior consultations with supervising authorities (as defined under the GDPR) or other competent data privacy authorities, if requested by the Customer or as otherwise required under the applicable Data Protection Laws.

8.3 The Customer will pay or reimburse the Company for the expenses and costs incurred by the Company in performing its obligations under clause 8.

9. Deletion and Return of Customer Data

9.1 Upon termination of this DPA, the Company will, in the discretion of the Customer either delete or return to the Customer all Customer Data in the possession of the Company.

9.2 The Company may retain:

a. Customer Data to the extent required by the Company to comply with applicable laws and only for such period as required by applicable laws.

b. documentation which serves as evidence of the orderly and accurate Processing of Customer Data by the Company.

9.3 If the Company retains Customer Data in accordance with clause 9.2 above, the Company's obligations under this DPA in respect of Processing Personal Data will apply to such retained Customer Data and will survive termination or expiry of the Head Contract.

10. Confidentiality

10.1 The Company will keep all Customer Data confidential and will not disclose such Customer Data to any third party without the Customer's prior written consent.

10.2 The Customer acknowledges and agrees that the Company is not in breach of clause 10.1, if the Company discloses Customer Data:

a. as permitted under this DPA; or

b. as required by applicable law or any court order, and provided the Company notifies the Customer of the required disclosure prior to making such disclosure, unless notification is prohibited by the applicable law or under the court order.

11. Evidence and audits

11.1 The Customer may from time to time (but not more than once annually) and at its own cost conduct an audit on the Company to verify the Company's compliance with this DPA or the applicable Data Protection Laws, by providing the Company at least 30 days' prior written notice.

11.2 If the Customer requests any such audit, the Company will provide any assistance reasonably required by the Customer to conduct the audit, including (without limitation) by providing the Customer access to any records relevant to the Company's Processing of Customer Data or the Company's premises within normal business hours (Mondays to Fridays from 9am to 5pm).

11.3 The Company is entitled, at its own discretion and taking into account the Customer's legal obligations, not to disclose information which is sensitive with regard to the Company's business or if the Company would be in breach of statutory or other contractual provisions as a result of its disclosure. The Customer is not entitled to get access to data or information about the Company's other customers, cost information, quality control and contract management reports, or any other confidential data of the Company that is not directly relevant for the agreed audit purposes.

11.4 If the Customer commissions a third party to carry out the audit, the Customer will obligate the third party in writing in the same way as the Customer is obliged vis-à-vis the Company according to this section 11. In addition, the Customer will by way of written agreement obligate the third party to maintain secrecy and confidentiality unless the third party is subject to a professional obligation of secrecy. At the request of the Company, the Customer will immediately submit to the Company the commitment and confidentiality agreements with the third party. The Customer may not commission any of the Company's competitors to carry out the audit.

11.5 At the discretion of the Company, proof of compliance with the obligations under this DPA may be provided, instead of an inspection, by submitting an appropriate current opinion or report from an independent authority (e.g. auditor, audit department, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification by IT security or data protection audit (the "Audit Report"), if the Audit Report makes it possible for the Customer in an appropriate manner to convince itself of the Company's compliance with the contractual obligations contained in this DPA.

12. Contract term and termination

12.1 The term and termination of this DPA will be governed by the term and termination provisions of the Head Agreement. A termination of the Head Agreement automatically results in a cancellation of this DPA. An isolated termination of this contract is excluded.

13. Liability

13.1 The Company's liability under this DPA will be governed by the disclaimers and limitations of liability provided for in the Head Agreement. As far as third parties assert claims against the Company which are caused by the Customer's culpable breach of this DPA or one of the Customer´s obligations as the controller in terms of Data Protection Laws, the Customer will upon first request indemnify and hold the Company harmless from these claims.

13.2 The Customer undertakes to indemnify the Company upon first request against all possible fines imposed on the Company corresponding to the Customer's part of responsibility for the infringement sanctioned by the fine.

14. Final provisions

14.1 In case individual provisions of this DPA are ineffective or become ineffective or contain a gap, the remaining provisions will remain unaffected. The Parties undertake to replace the ineffective provision by a legally permissible provision which comes closest to the purpose of the ineffective provision and that thereby satisfies the requirements of Art. 28 GDPR.

14.2 In case of conflicts between this DPA and other arrangements of the Parties, in particular the Head Agreement, the provisions of this DPA will prevail to the extent necessary to resolve the conflict or inconsistency.

Annex I – Parties, Selected Module, and Description of Transfer

A. Parties

	Data exporter	Data importer
Name	The party identified as the Customer in the Head Agreement	The party identified as the Company in the Head Agreement
Role	Controller	Processor
Business address	The Customer's address details as identified in the Head Agreement	**Asia Pacific HQ** 17 Henry Street, Spring Hill, Brisbane, QLD 4000, Australia **North America HQ** Office 639, 699 Burrard Street, Vancouver, BC V6C 2R7, Canada
Activities	Using the AutoRFP.ai platform to create, manage and submit responses to RFPs and other business proposals	Provision of an online RFP response platform with tools for creating, collaborating, and managing RFP responses; offering features based on AI and large language models for automated response generation
Key contact and details for privacy / data enquiries	The Customer's Key Contact as identified in the Head Agreement	Attn: Privacy Officer By email: info@autorfp.ai

B. Selected Module

Module in operation: Module 2.

C. Description of transfer

The following table provides further Information on the Processing of personal data comprised in Customer Data.

1	Purpose and extent of Data Processing and transfer	Provision of AutoRFP.ai online software as a web application and browser extension that functions as a platform for creating, collaborating, and managing RFP responses; Fulfil the Processor's obligations under the Contract. Tools based on large language models such as generative pre-trained transformer models ("GPT") may be used for response generation, automatically searching and writing responses to requirements.
2	Types of personal data	Contact data; usage data; any data filled in by the Customer in the Software, such as prompts; Employee Data; Customer Data; Supplier Data; User-generated Data; User data; Profile data; Usernames; password; email; logfiles.
3	Categories of data subjects	Users of AutoRFP.ai; and (only to the extent provided by or on behalf of an AutoRFP.ai user) such other data subjects mentioned or included in data filled in by the Customer in the Software.
4	Frequency of data transfer	Continuous, depending on the user's use of the Software.

5	Period of data retention	User data will be retained for the duration of the Customer's use of the Software and until the earlier of: ninety (90) days after the Customer deletes the applicable data from their account in the Software; or ninety (90) days after the Customer closes their account in the Software and requests account deletion. System logs and related operational data may be retained for longer periods as required for security, compliance, and troubleshooting purposes: ● Security and access logs: for up to twenty-four (24) months ● Transaction records: for up to seven (7) years (where required by law). Upon termination or expiration of the agreement, Customer Data may be retained in system backups that cannot reasonably be isolated for deletion. Such Customer Data will remain subject to the security and confidentiality provisions of the Head Agreement and will not be accessible through normal application functions. System backups are securely maintained with restricted access and are automatically purged according to AutoRFP.ai's standard backup rotation schedule (summary available on request).
6	Sensitive data transferred	None.

Annex II – Technical and Organisational Measures

Executive Summary

At AutoRFP.ai, we are deeply committed to the General Data Protection Regulation (GDPR) compliance, ensuring the protection and confidentiality of personal data. Our GDPR Technical and Organisational Measures (TOM) document outlines the stringent steps we've taken to align with GDPR requirements, focusing on confidentiality, integrity, availability and resilience, and regular review and evaluation of our practices.

Confidentiality: Our measures encompass physical and digital access controls, including stringent AWS data center security and multi-layered digital safeguards. We employ real-time security monitoring, two-factor authentication, strict access controls, and comprehensive encryption strategies.

Availability and Resilience: Our approach includes advanced availability controls, recoverability measures, and resilience and data retention strategies, ensuring continuous and secure data accessibility.

Regular Review, Assessment, and Evaluation: We regularly evaluate our security measures and policies, leveraging Firestore for secure, scalable data management and routine database backups for data integrity.

Certifications: Our infrastructure, managed by AWS, adheres to top-tier certifications, demonstrating our commitment to maintaining and enhancing our security posture.

By implementing these comprehensive measures, AutoRFP.ai provides a GDPR-compliant platform, safeguarding customer data with the highest level of security and privacy.

Table of Contents

1. Confidentiality

1.1 Physical Access Controls

- *Measures suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used.*
- *Measures for ensuring physical security of locations at which personal data are processed*

Datacenter (AWS)	
Access Is Scrutinised	AWS restricts physical access to people who need to be at a location for a justified business reason. Employees and vendors who need to be present at a data centre must first apply for access and provide a valid business justification. The request is reviewed by specially designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.
Entry Is Controlled And Monitored	Entering the Perimeter Layer is a controlled process. We staff our entry gates with security officers and employ supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they are given a badge requiring multi-factor authentication and limiting access to pre-approved areas.
AWS Data Center Workers Are Scrutinised, Too	AWS employees who routinely need access to a data centre are given permissions to relevant areas of the facility based on job function. But their access is regularly scrutinised, too. Staff lists are routinely reviewed by an area access manager to ensure each employee's authorisation is still necessary. If an employee doesn't have an ongoing business need to be at a data centre, they must go through the visitor process.
Monitoring For Unauthorised Entry	AWS employees are continuously watching for unauthorised entry on our property, using video surveillance, intrusion detection, and access log monitoring systems. Entrances are secured with devices that sound alarms if a door is forced or held open.
AWS Security Operations Centers Monitors Global Security	AWS Security Operations Centers are located around the world and are responsible for monitoring, triaging, and executing security programs for our data centers. They oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data center security teams. In short, they support our security with continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyse a potential security incident.
AutoRFP.ai Offices	
Entry Point Security	At AutoRFP.ai, we ensure the security of our

Datacenter (AWS)	
	premises with locked entry points. Access to our facilities is strictly controlled and monitored. Only authorised personnel with verified credentials can gain entry, ensuring a secure and controlled environment.
Visitor Management	This process ensures a detailed record of all non-employee entries and exits. Visitors are only allowed entry when accompanied by an authorised escort, guaranteeing oversight and maintaining the integrity of our secure areas.
No Unsupervised External Access	To safeguard our sensitive company information and maintain operational security, no external parties are permitted on site without an AutoRFP.ai employee escort. This policy is strictly enforced to ensure that all visitors are always under the supervision of a knowledgeable staff member.
Internal Information Control	In line with our commitment to data security and confidentiality, the printing of internal company information is strictly prohibited. This measure is in place to prevent unauthorised physical dissemination of sensitive data, further securing our intellectual property and client information.

1.2 Digital Access Controls

Measures suitable for preventing data processing systems from being used by unauthorised persons.

Technical Measures	Organisational Measures
Active Monitoring of Company Device compliance with policies via Drata Agent	**Regularly audited permission management**
Two-factor Authentication is enforced via Single Sign-On for all applications	**Strict access control**
Anti-Virus Software	
Firewall	
Intrusion Detection Systems	
Use of VPN for remote access	
Encryption of data carriers	
Automatic desktop lock	
Encryption of hard drives on workstations and laptops	

Internal Security

AutoRFP.ai has implemented several internal security controls to protect our systems and data.

Here are the key internal security controls that we have implemented:

1. **Real-Time Security Monitoring:** We have implemented real-time security monitoring to quickly identify and respond to potential security threats, reducing the risk of a successful attack.
2. **Multi-Factor Authentication:** We require multi-factor authentication to access our systems and data, helping prevent unauthorised access.
3. **Least Privilege Access:** We have implemented least privilege access controls to limit user access to only those systems and data necessary to perform their job functions, reducing the risk of unauthorised access or malicious actions.
4. **Patch Management:** We have a patch management program in place to ensure that our systems and applications are updated regularly with the latest security patches and fixes, reducing the risk of known vulnerabilities being exploited.
5. **Incident Response Planning:** We have developed an incident response plan to respond quickly and effectively to security incidents, reducing the risk of further compromise.
6. **End-to-End Encryption:** We use end-to-end encryption for sensitive organisational data to ensure that data is protected from unauthorised access and interception.

By implementing these internal security controls, we are confident in providing a secure platform for our customers. We understand the importance of security and take proactive measures to ensure the confidentiality, integrity, and availability of our systems and data.

Internal Policies & Procedures

AutoRFP.ai uses the Drata compliance system to follow ISO 27001:2022 standard. Some of the relevant policies to ensure confidentiality via Physical and Digital controls include:

- Encryption Policy
- Information Security Management System (ISMS) Plan
- Information Security Policy
- Password Policy
- Physical Security Policy
- System Access Control Policy
- Vulnerability Management Policy

Granular Access Controls

AutoRFP.ai granularly controls access to application resources, following least privilege principles. This means all URLs and API endpoints are limited to only those users who need to access them, further limiting the attack surface area of the application.

1.3 Separation Control

- *Measures that ensure data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.*

Technical Measures	Organisational Measures
API Layer Separation	Developing separate API endpoints for different data categories. Enforcing a clear boundary in data processing and access at the software level.
Dedicated Data Storage for Different Services	Utilising separate database schemas for services such as customer management, RFP processing, and internal operations. This ensures that data related to each service is stored and managed independently.
Service-Specific Data Handling	Implementing tailored data handling logic in our software. Ensuring that data collected for RFP responses is processed separately from customer contact information.

1.4 User Identification and Authorisation

- *Measures for user identification and authorisation*

AutoRFP.ai places a high priority on robust user identification and authorisation to maintain data confidentiality. This section outlines our comprehensive measures in this area, including the use of Google and Microsoft Single Sign-On (SSO) services.

User Identification Controls:

1. **SSO Integration with Google and Microsoft:** Utilises Single Sign-On integrations with Google and Microsoft for streamlined and secure user identification. This approach leverages the advanced security measures of these established platforms.
2. **Email Verification:** Implements mandatory email verification for all new accounts to confirm user identity.
3. **Account Authentication Logs:** Maintains logs of account authentication activities, enabling the monitoring of unusual or potentially unauthorised access attempts.

Authorisation Controls:

1. **Role-Based Access Control (RBAC):** Employs RBAC to grant access rights based on the user's role within the organisation. This ensures users have access only to the data and features necessary for their specific roles.
2. **Multi-Factor Authentication (MFA):** Requires MFA for all users, adding an additional layer of security. This is particularly enforced for accessing sensitive data or administrative functions.
3. **Regular Access Reviews:** Conducts periodic reviews and audits of user access rights to ensure that they are appropriate for the user's current role and responsibilities.

SSO Specific Measures:

1. **Encrypted Communication:** Ensures that all communications during the SSO process are encrypted, maintaining the security and integrity of user credentials.
2. **Automatic Session Timeout:** Implements automatic session timeouts for SSO sessions to reduce the risk of unauthorised access from unattended devices.
3. **Compliance with Security Standards:** Ensures that our SSO implementation complies with relevant security standards and best practices, including GDPR and other data protection regulations.

2. Integrity

2.1 Transfer Controls

- *Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.*

Technical Measures	Organisational Measures
Logging of accesses and retrievals	Survey of regular retrieval and transmission processes
Provision via encrypted connections with https	Data Protection Policy
Use of signature procedures (case dependent)	Information Security Policy
	Encryption Policy

Encryption in Transport

For data in transit, we use HTTPS encryption. This encrypts all data transmitted between our servers and users' devices, ensuring that unauthorized parties cannot intercept or access sensitive information.

Encryption at Rest

For data at rest, we use AES-256 encryption, one of the safest encryption methods. This ensures that all data stored on our servers is encrypted and cannot be accessed without proper authorisation.

Encryption for Sensitive Information

We implement the practice of salting sensitive information. When sensitive information, such as passwords, is salted, a random sequence of characters is added to the information before storing it in our databases. This makes it harder for hackers to use brute force attacks or precomputed tables to guess passwords.

2.2 Input Controls

- *Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems.*
- *Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).*

Technical Measures	Organisational Measures
Technical logging of the entry, modification and deletion of data	**Traceability of data entry, modification and deletion through individual user names (not user groups)**
	Assignment of rights to enter, change and delete data based on authorisation
	Retention of forms from which data has been transferred to automated processes
	Clear responsibilities for deletions
	Information Security Policy

2.3 Event Logging Controls

- *Measures for ensuring event logging*

1. **Comprehensive Logging System:** AutoRFP.ai Implements a robust logging system that records key events across our infrastructure. This includes user access events, system changes, network activity, and any anomalies detected.

2. **Real-Time Monitoring:** Utilises real-time monitoring tools to continuously track and analyse log data, enabling prompt detection and response to unusual activities or potential security threats.

3. **Log Integrity and Protection:** Ensures the integrity and security of log data through encryption and secure storage practices, preventing unauthorised access or tampering.

3. Availability and Resilience

3.1 Availability Control

- *Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).*

Technical Measures	Organisational Measures
Regular Software Updates and Patch Management	**Incident Response Plan**

Regular Data Backups	

3.2 Recoverability Control

- *Measures capable of quickly restoring personal data availability and access in the event of a physical or technical incident.*

Resilience & Data Retention

Our resilience and data retention policies ensure that we retain data in accordance with our legal and regulatory requirements. We have defined policies for hot data, which includes frequently accessed data, and cold data, which includes less frequently accessed data. This approach ensures that we are efficiently using our storage resources while ensuring that all data is retained for as long as required.

Point-in-time-Restores

We provide point-in-time restores every 60 seconds to enable our customers to recover data to a specific point in time. This feature allows our customers to recover data in case of accidental deletion or corruption.
By providing this feature, we help ensure that our customers' data is available when needed.

Contact: security@autorfp.ai

Annex III - List of Subprocessors

The Controller has authorised the use of the following Subprocessors:

Subprocessor	Description of processing	Location	Contact details
Infrastructure			
Amazon Web Services, Inc. (AWS)	The AutoRFP.ai online service is hosted and Customer Data is stored and processed on AWS.	United States, Germany or Australia (as selected by Customer in Order Form).	https://aws.amazon.com/compliance/gdpr-center/
Google LLC	Cloud hosting provider and translation assistance	United States, Germany or Australia (as selected by Customer in Order Form).	https://cloud.google.com/privacy/gdpr?hl=en
Microsoft Azure	AI services built into the application.	United States, Germany or Australia (as selected by Customer in Order Form).	https://www.microsoft.com/en-au/trust-center/privacy/gdpr-overview
Datadog, Inc.	AutoRFP.ai leverages Datadog for user experience analytics, optimizing interface design and customer interaction.	United States or Germany (as selected by Customer in Order Form).	https://www.datadoghq.com/gdpr/
Sales, Support & Billing			
Intercom, Inc.	AutoRFP.ai employs Intercom for streamlined customer support and communication.	United States	https://www.intercom.com/help/en/articles/1385437-how-intercom-complies-with-gdpr
Hubspot, Inc.	Customer relationship management and marketing automation.	United States	https://www.hubspot.com/data-privacy/gdpr
Stripe, Inc.	AutoRFP.ai integrates Stripe for secure payment processing.	United States	https://stripe.com/au/legal/privacy-center