Refapp's Data Privacy Agreement for Australian Clients

This document details Refapp's practices for protecting personal information and ensuring compliance with the **Australian Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)**. This statement is intended to assure our clients that our services enable them to meet their data protection obligations when using our SaaS platform for managing information related to candidates, referees, and recruiters.

Contractual Commitment (APP 8.1 & Section 16C)

- **Reasonable Steps:** Refapp contractually undertakes to handle all Personal Information in accordance with the Australian Privacy Principles (APPs).
- **Accountability**: This commitment constitutes "reasonable steps" under APP 8.1. Refapp acknowledges that it acts as an "Overseas Recipient" and accepts the flow-down of privacy obligations to ensure the Client remains protected under Section 16C of the Privacy Act.

Application of Australian Privacy Principles (APPs)

Refapp's security framework is structured to directly align with and support our clients' obligations under the APPs. Our commitment is to manage personal information in a manner that is open, transparent, and secure.

- **APP 11 – Security of Personal Information:** This principle requires us to take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. The measures detailed below demonstrate how we meet this obligation.
- **APP 1 – Open and Transparent Management**: We provide clear documentation, such as this statement, to ensure you are fully informed about our data handling and security practices.
- **APP 8 – Cross-border Disclosure:** We provide a list of our service providers and their data storage locations, ensuring you have the necessary information to manage your own obligations for cross-border data handling.
- **APP 12 & 13 – Access and Correction**: Our platform and support processes are built to assist you in fulfilling requests from individuals to access or correct their personal information, as required by the APPs.

Technical and Organisational Security Measures

Below is a summary of the key measures we have implemented to protect the personal information processed on our platform:

1. Data Protection

- **Encryption:** All data is encrypted both in transit (using industry-standard secure protocols like HTTPS) and at rest (via full database encryption). Critical personal data is also encrypted at the field level to provide an additional layer of protection.
- **Data Minimisation and Retention**: We use time-based data retention policies to ensure personal information is not stored longer than necessary. We anonymize data when aggregating it for reports, which further reduces the amount of identifiable information we hold.

2. System Integrity and Availability

- **Risk Management:** We conduct regular risk assessments, automated vulnerability scanning, and continuous monitoring to identify and address security threats proactively.
- **Resilience and Recovery**: We perform daily automated backups on physically separated sites. We have a defined disaster recovery process and conduct annual testing to ensure we can restore system infrastructure from scratch, which maintains the availability and resilience of your data.

3. Access Control and Accountability

- **User Identification and Authorization**: Access to our systems is secured with Multi-factor Authentication (MFA) and role-based access control, which restricts data access to authorized personnel only. We conduct annual user access reviews to ensure these controls remain effective.
- **Logging and Auditing**: All user and administrative activity is logged, providing a detailed audit trail. This allows us to monitor for any unauthorized access and supports accountability.
- **Personnel Training**: All our staff receive regular security training as part of our Information Security Management System (ISMS), promoting a consistent focus on data protection.

Data Breaches and the Notifiable Data Breaches (NDB) Scheme

Refapp's incident response plan is designed to support our clients' obligations under the Australian Notifiable Data Breaches (NDB) scheme.

- **Timely Notification:** In the event of a data breach, we will notify client within 24–48 hours of a suspected breach and will cooperate to complete an assessment within the statutory 30-day period.
- **Support for Assessment**: We will provide you with all necessary information to help you assess whether the breach is likely to result in "serious harm" to affected individuals, as required by Australian law.
- **Client's Obligation to Notify**: We will assist you in fulfilling your obligation to notify the affected individuals and the Office of the Australian Information Commissioner (OAIC) if a breach is deemed notifiable.

Service Providers and Data Location

A current list of our service providers and the locations where data is be stored is available. We ensure that any service provider we use is contractually required to maintain security standards that are consistent with our obligations to you under the Australian Privacy Act.

Conclusion

Refapp's security framework provides robust data protection that is specifically designed to support our clients' compliance with the Australian Privacy Act. This document confirms our commitment to managing personal information with care and security, allowing you to use our service confidently and meet your privacy obligations.