Acendre Privacy Policy

Table of Contents

1. Introduction and Scope

This Privacy Policy outlines how Acendre Pty Ltd ("**Acendre**", "**us**", "**we**") collects, holds, uses, and discloses personal information through the Acendre Recruit software-as-a-service platform ("Acendre Recruit" or the "Platform") when providing services to our clients.

We are committed to protecting the privacy of individuals whose personal information is processed through Acendre Recruit, in accordance with the Privacy Act 1988 (Cth) (the "**Privacy Act**"), including the Australian Privacy Principles ("**APPs**"), and the specific privacy and security requirements of our clients.

This policy applies specifically to personal information processed within the Acendre Recruit Platform as used by our clients. It explains our practices regarding the handling of personal information related to individuals applying for roles, client staff using the Platform for recruitment and HR purposes, and other individuals whose data may be entered into the system during the recruitment lifecycle.

It is important to understand that in the context of providing the Acendre Recruit application's functionality, we primarily act as a data processor. The client, as the data controller ("**APP Entity**"), determines the purposes and means of processing personal information. This policy is limited to our commitment as a data processor. Individuals should refer to the specific privacy policies of the relevant APP Entity for information on how that APP Entity handles your personal information.

This policy addresses the requirements of APP 1 (which relates to open and transparent management of personal information) by outlining:

- The types of personal information we collect and hold on behalf of clients.
- How we collect and hold personal information.
- The purposes for which we collect, hold, use, and disclose personal information.
- How individuals can access and seek correction of their personal information.
- How individuals can lodge a complaint about a breach of the APPs.
- If we disclose personal information to overseas recipients.

2. Types of Personal Information Collected and Held

Acendre, acting on behalf of our clients, collect and hold various types of personal information necessary for the functioning of the Acendre Recruit Platform and the recruitment processes managed by our clients. The specific types of information collected are determined by our client and their configuration of the Acendre Recruit Platform.

This information typically relates to job applicants, potential candidates, referees, and client personnel involved in the recruitment process. The types of personal information may include, but are not limited to:

Table 1: Examples of Personal Information Processed by Acendre Recruit

Category	Examples	Sensitivity Considerations
Identity & Contact	Name, address, email address, phone number, date of birth, employee ID (for client staff), citizenship/residency/visa status, gender identity.	Some data points (e.g., citizenship, potentially gender identity) may be sensitive or require careful handling.
Application Data	Resumes/CVs, cover letters, employment history, education/qualifications, certifications, responses to selection criteria, work samples, video interview recordings, psychometric assessment results.	Often contains detailed personal history. Video/assessment results can be considered sensitive.
Screening & Checks	Referee details and reports, background check results (e.g., police checks, working with children checks – often managed via integration), security clearance status/details.	This is highly sensitive data. Collection and use of the information is strictly governed by client policy and relevant laws.
Government Identifiers	Tax File Numbers (TFNs) and potentially other identifiers if configured by our client.	This data is subject to specific rules under the Privacy Act (APP 9) and TFN Rule 2015. Our Acendre Recruit Platform is designed to limit TFN collection where possible.
Sensitive Information	Information about racial or ethnic origin, health information (e.g., disability status for reasonable adjustments), criminal record, professional/trade association membership.	This data requires a higher level of protection required under the Privacy Act (APP 3). Collection requires consent unless an exception applies, managed by our client.
Platform Usage Data	User login details (client staff), audit logs of user activity, IP addresses, browser information, system interaction data.	Necessary for security, auditing, and system functionality.

The collection of sensitive information (as defined in the Privacy Act) and Government Related Identifiers ("**GRIs**") like TFNs is subject to stricter rules. We provide the Platform capabilities, but our client, as the data controller, is responsible for ensuring lawful collection of personal information, including obtaining necessary consents and providing appropriate notices. Our systems include controls to support how our clients meet these obligations, such as configurable fields and access restrictions.

3. How Personal Information is Collected and Held

Collection Methods

Personal information processed within the Acendre Recruit Platform is collected primarily through the following methods, directed by our client:

- **Directly from Individuals:** Applicants provide information when creating profiles, submitting applications, responding to questionnaires, or participating in assessments or interviews conducted via the Acendre Recruit Platform.
- **From Clients:** Client staff (e.g., HR personnel, hiring managers) input information about candidates, recruitment processes, or existing employees into the Acendre Recruit Platform.
- **From Third Parties:** Information may be collected from referees (provided by applicants), recruitment agencies engaged by the client, or providers of background checking and assessment services integrated with the Acendre Recruit Platform, based on authorisations managed by the client.
- **Automatically:** When individuals (applicants or client staff) interact with the Acendre Recruit Platform, technical data such as IP address, login times, and user actions may be logged automatically for security, auditing, and operational purposes.

We collect this information solely for the purpose of providing the Acendre Recruit service to our client, acting upon their instructions as documented in service agreements we enter with them.

Information Storage and Security

We are committed to protecting the personal information we hold on behalf of our clients from misuse, interference, loss, unauthorised access, modification, or disclosure, in line with the APP 11 requirements.

- **Data Sovereignty:** All client data processed through the Acendre Recruit Platform, including personal information, is hosted within Australia using Amazon Web Services ("**AWS**") facilities located in the Australian region. This ensures data remains within Australian jurisdiction, addressing key data sovereignty requirements for commonwealth government clients. No production data is stored or processed outside of Australia.
- **Security Framework Alignment:** We employ security measures designed to align with the Australian Government's Protective Security Policy Framework ("**PSPF**") and Information Security Manual ("**ISM**") requirements up to the PROTECTED level. This includes technical controls (e.g., encryption, access controls, network security) and organisational measures (e.g., personnel security, incident response planning).
- **Technical Security Measures:** Key measures include:
    - Encryption of data at rest and in transit using industry-standard protocols (e.g., TLS 1.2+, AES-256).
    - Robust access control mechanisms, including role-based access configured by the client, and multi-factor authentication options.
    - Regular security assessments, vulnerability scanning, and penetration testing.
    - Intrusion detection and prevention systems, logging, and monitoring.

    - Secure software development lifecycle practices.
- **Data Segregation**: Acendre supports both multi-tenant and dedicated infrastructure deployments. For clients on the multi-tenant Acendre Recruit Platform, client data is logically segregated using robust application-layer and database controls. For clients with dedicated infrastructure, data is physically segregated through separate infrastructure instances and configurations. In all cases, data segregation is enforced through access controls and isolation measures aligned with Australian Government ISM and PSPF guidelines.
- **Personnel Security:** Our personnel with access to the Platform environment undergo appropriate background checks and security training. Access is granted based on the principle of least privilege.
- **Data Retention and Destruction:** Personal information is retained within the Acendre Recruit Platform for periods determined by our client, in accordance with their record-keeping obligations (e.g., under the Archives Act 1983) and privacy policies. We securely destroy or de-identify personal information when instructed by our client or upon cessation of the service contract, following agreed procedures. Standard platform functionality allows clients to manage data retention rules.

4. Purposes for Which Information is Collected, Held, Used, and Disclosed

As a data processor, we collect, hold, use, and disclose personal information within the Acendre Recruit Platform strictly for the primary purpose of providing the recruitment and talent management services to the client, and for related secondary purposes directly connected to this service delivery. Our clients, as data controllers, determine the specific purposes for which personal information is processed through the Platform.

These purposes generally relate to managing the client's recruitment and hiring processes, including:

- **Facilitating Job Applications:** Enabling individuals to search for vacancies, create profiles, and submit applications.
- **Managing Recruitment Workflows:** Allowing client staff to advertise roles, screen applications, schedule interviews, manage candidate communication, conduct assessments, perform background checks (often via integrations), manage offers, and onboard new hires.
- **Talent Pooling:** Enabling clients to maintain pools of potential candidates for future vacancies (subject to appropriate consents and notices managed by the client).
- **Reporting and Analytics:** Providing clients with tools to generate reports on recruitment activities (e.g., time-to-hire, diversity metrics), typically using aggregated or de-identified data where appropriate.
- **System Operation and Maintenance:** Using information (particularly technical/usage data) for monitoring system performance, ensuring security, providing technical support, troubleshooting issues, and managing system upgrades.
- **Compliance and Auditing:** Enabling clients to meet their legal and regulatory obligations related to recruitment and record-keeping and facilitating audits of platform usage.

We will **not** use or disclose personal information processed on behalf of our client for our own purposes, such as marketing or product development unrelated to the contracted service, unless explicitly instructed or permitted by our client or required by law.

Disclosure of personal information held within the Acendre Recruit Platform is controlled by our client. We only disclose information as directed by our client (e.g., to integrated third-party service providers like background checkers, assessment providers, or other HR systems used by the entity) or as required by Australian law (e.g., in response to a valid subpoena or warrant). Any such disclosures required by law would be notified to our client where permissible.

5. Access and Correction of Personal Information

You have a right under the Privacy Act to request access to, and correction of, the personal information held about you.

As We hold personal information primarily as a data processor on behalf of our client, requests for access or correction should be directed to the relevant client in the first instance. The client is responsible for verifying the identity of the individual and processing the request in accordance with the APPs and their own procedures.

You can typically identify the relevant client from the job advertisement, application portal branding, or communications received during the recruitment process. Contact details for the client's Privacy Officer or relevant contact point are usually available on the client's website or privacy policy.

We will provide reasonable assistance to our clients to enable them to respond to access and correction requests from individuals whose data is held within the Acendre Recruit Platform. This includes providing tools within the Platform for authorised client personnel to search for, retrieve, amend, or extract personal information.

In the event a request for access or correction is made directly to Us, we will, where possible and appropriate:

- Identify the client on whose behalf the information is held.
- Forward the request to the designated contact person at the client for handling.
- Inform the individual that the request has been forwarded to the relevant client.

Contact details for our Privacy Officer are provided in Section 9 for general privacy enquiries, but specific access/correction requests concerning data held by a client of Acendre Recruit should be directed to that entity.

6. Handling Privacy Complaints

We take privacy complaints seriously and have procedures in place to manage them effectively and transparently, consistent with APP 1.

If an individual believes that We, or the handling of your personal information within the Acendre Recruit platform (as used by a client), may be involved in a breach of the Australian Privacy Principles or the Privacy Act, you are encouraged to take the following steps:

- **Contact the Client:** As the client is the data controller, complaints regarding the handling of personal information within their recruitment process should first be directed to their privacy officer or designated contact point. Their privacy officer is best placed to investigate the specific context of the information handling.
- **Contact Us:** If the complaint relates specifically to our role as a service provider (e.g., regarding platform security, data hosting, or actions taken directly by Acendre personnel) or if you are unsatisfied with the client's response where it involves our systems or services, you may contact our privacy officer directly using the details in Section 9.
    - Please provide sufficient detail about the complaint, including the client involved (if applicable), the nature of the concern, relevant dates, and desired outcome.
    - We will acknowledge receipt of the complaint promptly (usually within 5 business days).
    - We will investigate the complaint, which may involve liaising with the relevant client if the information is held on their behalf.
    - We aim to resolve complaints efficiently and will provide a written response outlining the investigation findings and any steps taken, typically within 30 days. If the matter is complex and requires more time, we will advise the individual of the delay and the expected timeframe.
- **Contact the Office of the Australian Information Commissioner ("OAIC"):** If you are not satisfied with the response received from both the client and/or us, or you believe the complaint has not been adequately addressed, you have the right to lodge a complaint with the OAIC.
    - **OAIC Contact Details:**
        - Online: www.oaic.gov.au/privacy/privacy-complaints/
        - Phone: 1300 363 992
        - Mail: GPO Box 5218, Sydney NSW 2001

We will cooperate fully with the OAIC in the resolution of any complaints.

7. Notifiable Data Breaches ("NDB") Scheme

We are committed to complying with the NDB scheme under Part IIIC of the Privacy Act. We have implemented procedures to detect, assess, and respond to potential data breaches involving personal information held on behalf of clients within the Acendre Recruit Platform.

A data breach occurs when personal information held by an entity is subject to unauthorised access, disclosure, or loss that is likely to result in serious harm to any of the individuals to whom the information relates.

- **Detection and Assessment:** We employ monitoring and security systems designed to detect potential data breaches. If a potential breach is identified affecting data held within Acendre

Recruit Platform, We will promptly investigate to determine the nature of the incident and assess whether it constitutes an "eligible data breach" under the NDB scheme.

- **Notification to Client:** As We act as a data processor, in the event of a potential or actual eligible data breach affecting a client's data, We will notify the affected client without undue delay. This notification will include details about the nature of the breach, the kinds of information involved, and the steps We are taking to contain and remediate the breach.
- **Notification to OAIC and Individuals:** The responsibility for notifying the OAIC and affected individuals under the NDB scheme generally rests with our client as the data controller holding the primary relationship with you. We will provide our client with all necessary information and assistance to enable them to meet their NDB obligations in a timely manner.
- **Containment and Remediation:** We will take all reasonable steps to contain any data breach, mitigate the risk of harm, and prevent recurrence.

8. Cross-border Disclosure of Personal Information

We are committed to ensuring that personal information processed through Acendre Recruit Platform for Australian commonwealth government clients remains within Australia, aligning with data sovereignty requirements.

All client production data, including personal information, is stored and processed within Australia ("**Australian AWS region(s)**")

Furthermore, all support services for the Acendre Recruit Platform provided by our personnel are delivered from within Australia. Our personnel located outside Australia do not have access to client data or the production environment hosting the Acendre Recruit Platform.

Therefore, we do not disclose personal information held within the Acendre Recruit Platform (as used by Australian clients) to any overseas recipients.

9. Policy Updates and Contact Information

Policy Updates

This Privacy Policy may be reviewed and updated from time to time to reflect changes in our practices, technology, or legal requirements. The latest version of this policy will always be available on our website or provided to our clients as appropriate. We encourage individuals and our clients to review this policy periodically. The “Revision History” table indicates when substantive changes were made.

Contact Information

For questions about this privacy policy, our privacy practices, or to lodge a privacy complaint directly with us, please contact our privacy officer:

- **Email:** privacy.au@acendre.com
- **Mail:** The Privacy Officer, Acendre Pty Ltd, Level 3, 600 Victoria St, Richmond VIC 3121

Please note, for requests regarding access to or correction of personal information held within a specific client's instance of Acendre Recruit, individuals should contact the relevant client directly in the first instance (see Section 5).

10. Document Control

Data Classification: OFFICAL: COMMERCIAL IN CONFIDENCE

Document Owner: John Baker

Document Approver: ISMS Owner

Date of Next Review: May 2026

11. Revision History

Version	Date of revision	Updated by	Description of change	Approval reference
0.1	2025-04-09	John Baker, Acendre	Document Creation	
0.2	2025-05-01	CBW Partners	Legal revisions	
0.3	2025-05-02	Mireille Abdo, Acendre	Minor edits	
1.0	2025-05-07	John Baker, Acendre	Amendments based on Acendre feedback.	ISWG, May 2025
1.1	2025-10-30	John Baker, Acendre	Applied Acendre Document Template	