HR CROWD

Privacy Statement

How HR Crowd collects, holds, uses and discloses personal information

Entity: HR Crowd Pty Ltd (ABN 66 665 648 439)
Applies to: hrcrowd.com, our products including CrowdComply, and our services
Governing law: Privacy Act 1988 (Cth) and the Australian Privacy Principles
Version: 1.0
Effective date: 29th August 2026

Contents

Privacy at a glance

This summary is provided for convenience. The full statement below sets out our complete position and prevails if there is any inconsistency.

Question	Short answer
Who are we?	HR Crowd Pty Ltd (ABN 66 665 648 439), an Australian SAP HCM solution delivery partner based in New South Wales, serving customers across Australia and New Zealand.
Whose information do we handle?	Mainly business contacts — people at our customers and prospective customers, website visitors, job applicants and our own personnel.
What about employee data in CrowdComply?	CrowdComply runs inside our customer's own SAP environment. The customer controls that data, not us. If you are an employee or contractor of one of our customers, contact your employer about your records in the first instance.
Do we ever see customer employee data?	Yes — but only where a customer separately engages us under a written agreement to implement, configure or support their environment, and only under their instructions and access controls. We do not routinely monitor, mine or review customer data.
Do we sell personal information?	No. We never sell or rent personal information.
Do we send data overseas?	Possibly — some of the cloud services we use to run our own business store data outside Australia. Section 9 names the countries.
How do I access or correct my information?	Email our Privacy Officer using the details in section 21. We respond within 30 days.
How do I complain?	Contact us first (section 19). If you are not satisfied, you can complain to the Office of the Australian Information Commissioner.

1. About this Privacy Statement

1.1 HR Crowd Pty Ltd (ABN 66 665 648 439) (HR Crowd, we, us, our) is committed to protecting the privacy of the individuals whose personal information we handle.

1.2 This Privacy Statement explains how we collect, hold, use and disclose personal information, how you can access and correct that information, and how you can make a privacy complaint. It is our privacy policy for the purposes of Australian Privacy Principle (APP) 1.

1.3 We handle personal information in accordance with the Privacy Act 1988 (Cth) (Privacy Act) and the APPs. Where we handle personal information about individuals in New Zealand, we also have regard to the Privacy Act 2020 (NZ). Where we handle personal data about individuals in the European Economic Area or the United Kingdom, section 20 applies.

1.4 This Privacy Statement applies to:

- our website at hrcrowd.com and any related pages, forms and campaigns;
- our dealings with customers, prospective customers, partners and suppliers;
- our products, including the CrowdComply accelerator for SAP SuccessFactors — as to which, see section 2; and
- our consulting, implementation, support and managed services engagements, where we are separately engaged to provide them under a written agreement.

1.5 It does not apply to third party websites, applications or services that we may link to, including the SAP Store and any SAP service. Those are governed by the relevant third party's own privacy policy.

2. Two very different roles — and why it matters

> **The key point** For our own business information we decide how personal information is handled. For personal information inside a customer's SAP environment, the customer decides — we only ever act on that customer's instructions.

2.1 When we act for ourselves. We collect and handle personal information for our own purposes — for example, business contact details of the people we deal with at our customers and prospects, information from our website, and information from people who apply to work with us. For that information we are the entity responsible under the Privacy Act (an "APP entity"), and this Privacy Statement describes how we handle it.

2.2 When we act for a customer. CrowdComply is an accelerator that is deployed into our customer's own SAP SuccessFactors and SAP Business Technology Platform environment. The personal information processed in it — employee, contractor, contingent worker and candidate records, licences, certifications, authorisations and supporting documents — is collected, held and controlled by the customer, in the customer's own systems, under the customer's own privacy policy.

2.3 In that context:

- the customer is the entity responsible for that personal information (the APP entity, or the "controller" under other data protection laws);
- HR Crowd is a service provider, and acts only on the customer's documented instructions;
- we do not host, operate or control the customer's environment;
- we do not preview, screen, monitor, review, mine or analyse customer data as a matter of course; and
- we do not use customer data for our own purposes, and we never use it to train artificial intelligence or machine learning models.

2.4 If you are an employee, contractor or candidate of an organisation that uses CrowdComply. Your employer or engaging organisation is the right first point of contact about your records. They control what information is held, who can see it, how long it is kept, and how requests for access and correction are handled. If you contact us directly about such information, we will ordinarily refer you to that organisation, and will tell you that we have done so.

3. What personal information we collect and hold

3.1 Information we collect for our own purposes. The kinds of personal information we collect and hold include:

Category	Examples
Business contact information	Name, job title, role, employer, business email address, business phone number, business postal address, LinkedIn profile.
Relationship and engagement information	Records of meetings, calls, emails and correspondence; notes of your requirements and interests; event and webinar attendance; marketing preferences and subscription status.
Commercial information	Contract, order, quotation and invoicing details; billing contacts; payment records. We do not store full payment card numbers — card payments are processed by our payment providers.

Category	Examples
Support and service information	Requests, tickets, incident reports, screenshots, logs and correspondence you send us in connection with a service we are separately engaged to provide. These may incidentally contain personal information.
Website and technical information	IP address, approximate location derived from IP address, device and browser type, operating system, referring page, pages viewed, time and duration of visit, and information collected via cookies and similar technologies.
Recruitment information	Where you apply for a role with us: your resume, cover letter, employment and education history, qualifications, right-to-work status, referee details, interview notes and assessment results.
Personnel information	Where you work for or with us: information necessary to manage the engagement, including contact, payroll, tax, superannuation and performance information.

3.1A Our own employee records. Personal information we hold about our own current and former employees, where it directly relates to their employment relationship with us, is generally exempt from the Privacy Act under section 7B(3). We handle it in accordance with our internal policies and applicable workplace laws. Sections 17 and 18 of this Privacy Statement do not extend to those records.

3.2 Sensitive information. We do not generally seek or collect sensitive information (as defined in the Privacy Act) about the individuals we deal with in a business context. Where sensitive information is necessary — for example, a police check, health or accessibility information relevant to a recruitment or site access requirement — we collect it only with consent or where otherwise permitted by law, and we handle it with additional protections.

3.3 Information inside customer environments. Personal information held in a customer's CrowdComply deployment is collected and controlled by that customer, not by us. Depending on how the customer configures the solution, it may include sensitive information — for example, health-related fitness-for-work information, criminal record information relevant to site access, or membership of a professional or industrial association. The customer determines what is collected and is responsible for its lawfulness. See section 2 and section 6.

3.4 Unsolicited personal information. If we receive personal information that we did not solicit and could not lawfully have collected, we will destroy or de-identify it as soon as practicable, provided it is lawful and reasonable to do so.

4. How we collect personal information

4.1 Wherever reasonably practicable, we collect personal information directly from you. We collect it:

- when you contact us, enquire about our services, request a demonstration, or complete a form on our website;
- when you engage with us as a customer, prospect, partner, supplier or their representative — including through meetings, calls, emails and project work;
- when you subscribe to our updates, register for an event or webinar, or download content;
- when you raise a request or report an issue under a services agreement we have with you or your organisation;
- when you apply for a role with us, or are referred to us by a recruiter;
- automatically, when you visit our website, through cookies, log files and analytics tools (see section 13); and

- through our business systems, including our customer relationship management, marketing, email and collaboration platforms.

4.2 Collection from third parties. Where it is unreasonable or impracticable to collect directly from you, we may collect your personal information from: your employer or the organisation you represent; our customers and partners; SAP and other technology partners, including through SAP Store and partner referral programs; recruiters; publicly available sources such as company websites, professional networking sites and business registers; and business information and data enrichment providers. If we collect your information from someone else, we will take reasonable steps to notify you or otherwise make you aware of the matters set out in APP 5.

4.3 Access to customer environments. Where a customer engages us to implement, configure, integrate, test or support CrowdComply or another solution, that customer may provision access for our personnel to its systems. Any personal information our personnel encounter in that context is accessed under the customer's instructions and access controls, and is dealt with under section 6.

5. Why we collect, hold, use and disclose personal information

5.1 We collect, hold, use and disclose personal information for the following purposes:

- to respond to your enquiries and provide information you have requested;
- to supply, deliver, license, invoice and administer our products and services, including CrowdComply;
- to perform consulting, implementation, configuration, integration and support services under our contracts;
- to manage our relationship with customers, prospects, partners and suppliers, including account management and contract administration;
- to operate, secure, maintain and improve our website, systems and products;
- for marketing and business development, including sending updates, insights, invitations and product information, subject to section 14;
- to recruit, assess and onboard personnel;
- to manage risk, investigate and prevent fraud, misuse and security incidents;
- to comply with our legal, regulatory, tax, accounting and record-keeping obligations, and to respond to lawful requests from regulators, courts and law enforcement; and
- to establish, exercise or defend legal claims.

5.2 We will only use or disclose personal information for a secondary purpose where you would reasonably expect it and it is related to the primary purpose (or, for sensitive information, directly related), where you have consented, or where the use or disclosure is otherwise required or authorised by law.

5.3 Consequences of not providing information. You are not obliged to provide us with personal information. However, if you choose not to, we may not be able to respond to your enquiry, provide our products or services, deliver a project, process a support request, or consider your application for a role.

6. Personal information in customer environments

6.1 Where a customer separately engages HR Crowd under a written agreement to implement, configure, extend, test, migrate data into, or support CrowdComply or any other SAP solution, our personnel may be granted access to that customer's environment and may have access to personal information held in it, including employee and contractor records and supporting documents.

6.2 When that happens, we apply the following controls:

- Instruction-bound. We access and use that information only to perform the services the customer has engaged us to perform, and only in accordance with the customer's documented instructions and the applicable statement of work or data processing terms.
- Least privilege. Access is granted only to the personnel who require it for the engagement, at the minimum level of privilege necessary, and is revoked when the engagement ends or the need ceases.
- Customer-controlled. Access is provisioned, approved, reviewed and revoked by the customer within its own systems. The customer determines what our personnel can see.
- De-identified data preferred. Where the customer makes suitably masked, anonymised or synthetic test data available and it is fit for purpose, we will use it in preference to production data.
- No secondary use. We do not use customer data for our own purposes, for benchmarking, for marketing, for product development or to train artificial intelligence or machine learning models.
- No routine review. We do not preview, screen, monitor or review customer data other than as necessary to perform the engaged services.
- Confidentiality and training. Our personnel are bound by written confidentiality obligations and receive privacy and security awareness training.
- Records stay in place. Wherever possible we work within the customer's environment rather than extracting data. Where extraction is unavoidable — for example, for defect reproduction — we agree the scope with the customer, minimise the data, and delete it when it is no longer needed.

6.3 Responsibility for that information rests with the customer, including determining the lawful basis for collection, providing collection notices, obtaining consents, setting retention periods, configuring access and visibility controls, responding to individual requests, and assessing and notifying eligible data breaches.

7. How we hold and protect personal information

7.1 We hold personal information in electronic form in our business systems and in reputable cloud services, and, to a limited extent, in physical form. We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

7.2 Those steps include technical and organisational measures such as:

- access controls based on role and business need, with least-privilege provisioning and periodic review;
- multi-factor authentication on business systems and administrative accounts;
- encryption of data in transit and, for our cloud services, encryption at rest;
- endpoint protection, patching and vulnerability management on managed devices;
- logging and monitoring of access to systems holding personal information;
- confidentiality obligations, background checks where appropriate, and privacy and security training for personnel;
- contractual protections with our service providers, including obligations to protect personal information and to notify us of incidents;
- secure disposal and destruction procedures; and
- a documented data breach response plan (see section 16).

7.3 No method of transmission or storage is completely secure. While we take reasonable steps, we cannot guarantee absolute security.

8. Who we disclose personal information to

8.1 We may disclose personal information to:

Recipient	Purpose
Our personnel and contractors	To perform the purposes described in section 5.
Cloud and IT service providers	Hosting, email, collaboration, document management, file transfer, identity and endpoint security, and backup services.
Customer relationship and marketing platforms	Managing our customer and prospect relationships and sending communications you have subscribed to.
Support and ticketing platforms	Recording and managing support and project requests.
Accounting, invoicing and payment providers	Billing, collections and financial record keeping.
Analytics providers	Understanding how our website is used (see section 13).
Technology partners, including SAP	Where necessary to register a deal, arrange licensing or entitlements, log a product issue, or fulfil an order placed through the SAP Store. We disclose business contact details only, not customer employee data.
Professional advisers	Legal, accounting, audit and insurance advice.
Purchasers or investors	In connection with an actual or proposed sale, merger or restructure of our business, subject to confidentiality.
Regulators, courts and law enforcement	Where required or authorised by law, or to protect our legal rights.

8.2 We do not sell, rent or trade personal information, and we do not disclose personal information to third parties for their own direct marketing purposes.

8.3 We take reasonable steps to ensure that our service providers only handle personal information for the purposes we engage them for, and are bound by appropriate confidentiality and security obligations.

9. Overseas disclosure

9.1 Some of the cloud services we use to run our own business store or process personal information outside Australia. Based on our current arrangements, personal information we hold may be accessible in, or transferred to, the following countries:

Country or region	Reason
Australia	Our primary operating location and preferred data residency for our own systems.
New Zealand	Customers, personnel and project delivery in New Zealand.
United States	Cloud infrastructure, collaboration, marketing, analytics and support platforms operated by global providers.
European Union and United Kingdom	Certain vendor support, hosting and administration functions.
Singapore and other Asia-Pacific locations	Regional cloud infrastructure and vendor support functions used by some of our providers.

9.2 Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information — principally through contractual commitments that bind the recipient to APP-equivalent standards, vendor due diligence, and selecting providers with recognised security certifications such as ISO/IEC 27001 or SOC 2. Where we disclose personal information overseas, we generally remain accountable under section 16C of the Privacy Act for the recipient's handling of it. If we ever rely on an exception in APP 8.2 — for example, your express and informed consent under APP 8.2(b) — we will tell you before the disclosure that APP 8.1 will not apply to it.

9.3 Customer environments. The location of a customer's own SAP SuccessFactors and SAP Business Technology Platform data centres is determined by the customer and SAP, not by HR Crowd. Customers should consult their agreements with SAP for data residency information. Where our personnel access a customer environment from Australia or New Zealand to perform services, that access occurs from those countries.

9.4 This list may change as our service providers change. We review it when we update this Privacy Statement.

10. Data quality

10.1 We take reasonable steps to ensure that the personal information we collect, use and disclose is accurate, up to date, complete and relevant. We rely in part on you to tell us when your details change — please contact us using the details in section 21 if they do.

11. Retention and destruction

11.1 We retain personal information only for as long as we need it for the purposes described in this Privacy Statement, or for as long as we are required to retain it by law.

11.2 Indicative retention periods for information we hold for our own purposes are:

Information	Indicative retention period
Customer and contract records	For the term of the engagement and then 7 years, consistent with tax, corporations and limitation period requirements.
Prospect and marketing contact records	While the relationship is active, and for up to 2 years after the last meaningful engagement, unless you unsubscribe or ask us to delete earlier.
Support and project records	For the term of the engagement and then up to 7 years.
Unsuccessful job applications	Up to 12 months after the recruitment process concludes, unless you consent to us keeping your details longer.
Website analytics and log data	Up to 26 months, or the shorter period set in the relevant platform.

11.3 When we no longer need personal information, and we are not required by law to retain it, we destroy it or de-identify it using secure methods.

11.4 Retention of personal information inside a customer's CrowdComply deployment is determined and applied by that customer.

12. Anonymity and pseudonymity

12.1 You have the option of dealing with us anonymously or using a pseudonym — for example, when making a general enquiry, browsing our website, or providing feedback. We will accommodate this where

it is lawful and practicable. It will not be practicable where we need to identify you to provide a service, perform a contract, respond to a support request, consider a job application, or meet a legal obligation.

13. Cookies, analytics and our website

13.1 Our website uses cookies and similar technologies. Cookies are small files placed on your device that allow the site to function, remember your preferences, and help us understand how the site is used.

13.2 We use:

- strictly necessary cookies, which are required for the website to operate securely;
- preference cookies, which remember choices you make; and
- analytics and performance cookies, which help us understand how visitors find and use our site so we can improve it.

13.3 We may also use marketing and remarketing technologies to measure the effectiveness of our campaigns and to show relevant content to people who have visited our site.

13.4 You can control cookies through your browser settings and, where we provide one, through the cookie preference tool on our website. Blocking some cookies may affect how the website works.

13.5 Our website may contain links to third party websites, including the SAP Store, LinkedIn and other platforms. We are not responsible for the privacy practices of those sites.

14. Direct marketing

14.1 We may send you marketing communications about our products, services, insights and events where you have subscribed, where you are an existing customer or business contact and would reasonably expect to receive them, or where you have otherwise consented.

14.2 Every marketing email we send contains an unsubscribe link. You can also opt out at any time by contacting us using the details in section 21. We will action your request promptly and at no cost.

14.3 If you ask us to, we will tell you where we obtained your information.

14.4 We do not use or disclose sensitive information for direct marketing without your consent.

15. Automated decision-making

15.1 We do not use automated decision-making, including artificial intelligence, to make decisions about individuals that could significantly affect their rights or interests in the course of our own business. Decisions about customers, suppliers and job applicants are made by people.

15.2 CrowdComply applies rules configured by our customer to compare the credentials, licences, certifications and authorisations recorded against a worker with the requirements defined for their role, and to display a status and generate alerts. It is an information tool. It does not make employment, engagement, disciplinary, remuneration or work allocation decisions. Any decision about a worker — including whether to assign work, grant site access or take any other action — is made by the customer, by people, using CrowdComply as one input among others.

15.3 Where a customer configures CrowdComply in a way that contributes to decisions about individuals, the customer is responsible for meeting its own transparency obligations to those individuals, including the automated decision-making disclosure requirements that take effect under APP 1.7 on 10 December 2026.

15.4 We will review this section before 10 December 2026 and will update it if our practices change.

16. Data breaches

16.1 We maintain a data breach response plan. If we suspect a data breach involving personal information we hold, we will contain it, assess it, and take steps to prevent it recurring.

16.2 Where a data breach we are responsible for is likely to result in serious harm to any individual, and the Notifiable Data Breaches scheme in Part IIIC of the Privacy Act applies, we will notify the Office of the Australian Information Commissioner (OAIC) and the affected individuals as soon as practicable, including recommendations about the steps they should take. We will complete any assessment of a suspected eligible data breach within 30 days.

16.3 If we become aware of an incident affecting personal information within a customer's environment, or caused by our acts or omissions in performing services for a customer, we will notify that customer without undue delay and provide reasonable assistance so the customer can assess the incident and meet its own notification obligations. Where both we and the customer hold the affected information, we will agree which of us notifies under section 26WM of the Privacy Act. Otherwise, responsibility for assessing and notifying an eligible data breach affecting a customer's own records rests with the customer.

17. Access to your personal information

17.1 You may request access to the personal information we hold about you by contacting our Privacy Officer using the details in section 21.

17.2 We will need to verify your identity before we provide access. We will respond within 30 days. We do not charge for making a request; we may charge a reasonable cost-based fee for giving access where a request requires substantial work, and we will tell you before we do.

17.3 There are limited circumstances in which we may refuse access — for example, where giving access would have an unreasonable impact on the privacy of others, would reveal commercially sensitive information, would prejudice a legal claim or an investigation, or where the request is frivolous or vexatious. If we refuse, we will tell you why in writing and explain how to complain.

17.4 If your request relates to records held in an employer's CrowdComply deployment, we will refer you to that organisation, which controls those records.

18. Correcting your personal information

18.1 If you believe personal information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, you may ask us to correct it. Contact our Privacy Officer using the details in section 21.

18.2 We will take reasonable steps to correct the information within 30 days. If we have disclosed the information to others and you ask us to, we will take reasonable steps to notify them of the correction.

18.3 If we decide not to correct the information, we will tell you why in writing, explain how to complain, and — if you ask — attach a statement to the record noting that you believe it is inaccurate.

19. Complaints

19.1 If you have a concern or complaint about how we have handled your personal information, please tell us. Contact our Privacy Officer using the details in section 21, and describe the issue and how you would like it resolved.

19.2 We will acknowledge your complaint within 5 business days and aim to resolve it within 30 days. If we need longer, we will tell you why and keep you updated. We will tell you the outcome and our reasons in writing.

19.3 If you are not satisfied with our response, you may complain to the Office of the Australian Information Commissioner:

Contact method	Detail
Website	oaic.gov.au
Phone	1300 363 992
Post	GPO Box 5218, Sydney NSW 2001

19.4 Individuals in New Zealand may complain to the Office of the Privacy Commissioner (privacy.org.nz).

20. Other jurisdictions

20.1 New Zealand. Where we handle personal information about individuals in New Zealand, we do so in accordance with the Privacy Act 2020 (NZ) and the Information Privacy Principles, in addition to the APPs.

20.2 European Economic Area and United Kingdom. Where the EU or UK General Data Protection Regulation applies to our handling of personal data:

- our lawful bases for processing are generally: performance of a contract; our legitimate interests in operating, marketing and securing our business, balanced against your interests; compliance with a legal obligation; and, where relevant, your consent;
- you have the rights of access, rectification, erasure, restriction, portability and objection, and the right to withdraw consent at any time;
- transfers of personal data outside the EEA or UK are made under an adequacy decision or standard contractual clauses, together with supplementary measures where required; and
- you may lodge a complaint with your local supervisory authority.

20.3 Where we act as a processor for a customer, the customer's own arrangements and any data processing addendum agreed with us govern that processing.

21. How to contact us

Item	Detail
Legal entity	HR Crowd Pty Ltd
ABN	66 665 648 439
ACN	665 648 439
Privacy Officer	Adrian Everett. Co-CEO
Email	Adrian.everett@hrcrowd.com
Phone	1300 HR CROWD
Post	Privacy Officer, HR Crowd Pty Ltd, 6 Middlemiss Street, Lavender Bay, NSW, Australia
Website	hrcrowd.com

22. Changes to this Privacy Statement

22.1 We review this Privacy Statement regularly and may update it to reflect changes in our practices, our products, our service providers or the law. The current version is always available at hrcrowd.com.

22.2 Where a change is material, we will take reasonable steps to bring it to the attention of affected individuals, for example by a notice on our website or by email.

22.3 Version history:

Version	Date	Summary of change
1.0	[Insert date of publication]	First published.

This Privacy Statement is published at [insert public URL] and is the privacy statement referred to in the CrowdComply listing on the SAP Store.