Corporate Data and Personal Privacy Policy

Effective Date: 2025

Approved By: The Directors, Ulara Resources Pty Ltd

Contact: info@ulararesources.com.au

1. Purpose and Scope

Ulara Resources Pty Ltd ("Ulara", "we", "our", "us") is committed to protecting the privacy, confidentiality, and security of all corporate data and personal information it manages. This policy outlines how Ulara collects, stores, uses, discloses, and secures information relating to employees, contractors, clients, suppliers, and business partners, as well as corporate and operational data generated in the course of business.

This policy applies to all Ulara employees, contractors, consultants, and third-party service providers with access to company systems or data.

2. Definitions

- Corporate Data: All business, operational, financial, and technical information created, collected, or processed by Ulara, regardless of format (e.g., documents, databases, emails, intellectual property, analytics, or system logs).
- Personal Information: Information or an opinion about an identifiable individual, including names, contact details, identification numbers, employment or financial details, and other personal data as defined by the Privacy Act 1988 (Cth).
- Sensitive Information: Data relating to health, ethnicity, criminal records, or union membership, handled under higher protection standards.
- Data Breach: Any unauthorised access, disclosure, or loss of personal or corporate information.

3. Data Collection and Use

3.1 Personal Information

Ulara collects personal information that is reasonably necessary to manage employment, recruitment, client relationships, and service delivery. This includes employee and contractor details, prospective employee information, customer and supplier contact details, site visitor or incident records, and information provided by clients or business partners for legitimate service purposes.

Personal data is collected directly from individuals where possible, or through authorised third parties (e.g., background checks or referees).

3.2 Corporate Data

Corporate data is collected and created through normal business operations. This may include financial records, internal reports, analytics, client and project documentation, technical system logs, and intellectual property. Corporate data remains the property of Ulara and must be managed, stored, and transmitted in accordance with this policy.

4. Use and Disclosure

Ulara uses and discloses personal and corporate data only for legitimate business purposes, including employment management, client and supplier engagement, compliance, security monitoring, and business improvement.

Disclosure to third parties will occur only under secure, lawful, and contractual arrangements that ensure compliance with this policy and relevant privacy legislation.

5. Data Storage and Security

Ulara maintains both physical and electronic records in secure environments. Data may be stored in Australia or overseas through trusted providers that meet equivalent data protection standards.

5.1 Client Data Handling and Confidentiality

Ulara applies the same level of care, security, and privacy protection to client data as it does to its own corporate and personal information.

Client data refers to any information, records, or materials—whether personal, operational, financial, or technical—provided to Ulara by a client, or generated on a client's behalf during the course of business.

We ensure client data is accessed only by authorised personnel, stored and processed securely, and shared only under confidentiality and legal compliance obligations. Ulara does not sell, disclose, or otherwise share client data without consent, except where required by law.

5.2 Data Security Measures

We take reasonable steps to protect data against unauthorised access, misuse, interference, or loss, including encryption, access control, and secure infrastructure, and regularly review vendor compliance.

5.3 Secure Infrastructure and Access Controls

All staff and contractors must complete data protection training and follow cybersecurity protocols. Access to systems is role-based and subject to monitoring and audit logging.

6. Data Retention and Disposal

Personal and corporate data will be retained only as long as required for business or legal purposes. When no longer required, Ulara will securely delete or anonymise electronic data, destroy physical records, and ensure third-party data destruction meets equivalent standards.

7. Data Access and Correction

Individuals may request access to or correction of their personal information held by Ulara by contacting info@ulararesources.com.au. We will respond within a reasonable timeframe and may verify identity before granting access or making amendments.

8. Cross-Border Data Transfers

Where data is stored or processed offshore, Ulara ensures that the receiving party operates under privacy laws substantially similar to the Australian Privacy Principles (APPs) or under contractual safeguards. Common jurisdictions include Australia, the United States, and Canada.

9. Data Breach Response

Ulara maintains a Data Breach Response Plan to ensure prompt identification, containment, and notification of breaches. If a notifiable breach occurs under the Notifiable Data Breaches Scheme (NDB), affected individuals and the Office of the Australian Information Commissioner (OAIC) will be notified accordingly.

10. Policy Governance and Updates

This policy is reviewed annually or following significant legislative or operational changes. Updates will be published on Ulara's website, and all employees and contractors will be notified of material changes.

11. Complaints and Enquiries

If you have a concern regarding how Ulara has handled your information, please contact:
The Directors, Ulara Resources Pty Ltd
Suite 402, Building A, 11 Solent Circuit, Norwest, NSW 2153, Australia
Email: info@ulararesources.com.au
If unresolved, you may contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au.