ANINDILYAKWA ROYALTIES
Aboriginal Corporation

T: 07 4031 4125
ICN: 8394 ABN: 69 806 855 472

P: GPO Box 2644
Darwin NT 0801
A: Suite 4, Level 1, 101 Mitchell Street
Darwin NT 0800
E: admin@arac.com.au

Anindilyakwa Royalties Aboriginal Corporation (ARAC) Privacy Policy

Scope

The purpose of this policy is to ensure Anindilyakwa Royalties Aboriginal Corporation (ARAC) can collect personal information necessary for its purposes and functions, while recognising the right of individuals to have their information handled in ways that meet legal requirements, and that they would reasonably expect.

Context

ARAC is committed to protecting the personal information that we collect, hold, use and disclose. This policy enables ARAC to collect information and protects the right of the individual to privacy. It is to be used in conjunction with ARAC's Information Management and Information Security policies.

The *Privacy Act 1988* protects and regulates the collection, holding, use and disclosure of an individual's personal information and sensitive information. The core obligations in the Privacy Act are set out in the Australian Privacy Principles (found in Schedule 1 to the Act).

The Privacy Act defines 'personal information' to mean information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether recorded in a material form or not. The Privacy Act defines 'sensitive information' to include personal information about an individual's racial or ethnic origin, religious beliefs or affiliations, sexual orientation or practices or criminal record.

Policy

Any personal information collected or obtained by ARAC is collected, stored, and used only in accordance with the Privacy Laws, pursuant to section 5(7) of the *Information Act (NT).* ARAC will not access, use, disclose or retain any personal information as defined in *section 5(7) of the Information Act (NT)* except in performing their duties under this Policy.

Collection of Personal Information

ARAC will only collect personal information required to:

- Administer subleases or licenses under the township lease;
- communicate with the individual about ARAC activities, services, updates and opportunities; and/or
- complete processes or assessments, and/or deliver services or activities that the individual is contributing to or may be a beneficiary of.

ARAC will only collect personal information in a lawful manner as a result of the direct or implied consent provided by the individual via the individual's physical, verbal or digital interaction with ARAC as an organisation, its Board of Directors, employees or contractors, and where individuals have the opportunity to access the ARAC Privacy Policy.

Use of Personal Information

When personal information is collected from an individual, ARAC will take reasonable steps to ensure that personal information is used only for the purpose for which it was collected.

Personal information collected by ARAC can be used for a secondary purpose other than the above if:

- the individual consents;
- the individual would reasonably expect ARAC to use or disclose the information for a secondary purpose, and the secondary purpose is related to the primary purpose;
- the secondary use of the personal information is required or authorised by or under an Australian law;
- a permitted general situation exists in relation to the secondary use of the information;
- a permitted health situation exists in relation to the secondary use of the personal information; or
- ARAC has a reasonable belief that the secondary use is necessary for one or more enforcement related activities conducted by an enforcement body.

ARAC commits that its Directors and workers will only access personal information held by ARAC where it relates to the discharge of duties or responsibilities related to their employment.

Disclosure of Personal Information

ARAC commits not to disclose an individual's personal information to any other party except in the following circumstances:

- where the use or disclosure is required or authorised by law; and/or
- in order to store data with third party software providers utilised by ARAC for the purposes of data capture, storage and or communication, in which case the third party shall be bound by suitable undertakings to maintain such confidentiality.

While ARAC will require suitable undertakings from its providers, ARAC will not accept liability for the actions of third party software providers utilised by ARAC for data capture, storage and or communication. The direct or implied consent of an individual for ARAC to collect an individual's personal information is done so with this in mind.

Data Security

ARAC shall take all reasonable steps to protect the personal information held in its possession against loss, unauthorised access, use, modification, disclosure or misuse. Data is stored and kept secure in line with ARAC's Information Management and Information Security policies.

Where there is suspicion of a data breach the ARAC Executive Officer (EO) and IT Support are to be notified immediately; and a reasonable and expeditious assessment must be carried out immediately of becoming aware of the possible breach as to whether the breach is in fact an eligible data breach.

Action must also be immediately taken to contain the breach, whether the breach is determined to be an eligible breach or not and review whether any action can be taken to prevent future breaches.

An eligible data breach occurs when the following criteria are met:

- there is unauthorised access to or disclosure of personal information held by ARAC;
- the breach is likely to result in serious harm to any of the individuals to whom the information relates; and
- ARAC had been unable to prevent the likely risk of serious harm with remedial action.
- Where an eligible data breach has occurred, the following process must be followed in line with requirements of the Privacy Act:
- The employee/s who identified the risk must immediately notify the EO, who will then notify IT and the Board. The notification must include information about the time and date the suspected breach was discovered, the type of

information involved, the cause and extent of the breach, and the context of the affected information and the breach.

- The EO will assess and determine whether an eligible data breach has occurred.
- If unable to establish whether an eligible data breach has occurred, the EO in the first instance should engage ARAC's IT support.
- If it is determined that a data breach has occurred, the EO must immediately notify the following parties:
    - ARAC's insurance provider to address the breach and implement any required incident response actions;
    - the Office of the Australia Information Commissioner; and
    - any parties who are at risk because of the breach of information.

If the assessment is inconclusive as to whether the breach is an eligible data breach, ARAC encourages the above process to be followed as part of risk mitigation.

If the assessment shows the breach was not an eligible data breach, no further action is required.

Access or correction of personal information

ARAC must take reasonable steps to ensure personal information it holds is accurate, up-to-date, complete, relevant and not misleading and has regard to the purpose for which it is held. Individuals have the right to request access to personal information ARAC holds about them or to correct it. In accordance with the Australian Privacy Principles guidelines, ARAC must respond to a request to correct a record or to associate a statement within 30 calendar days of the request being received.

Disposal of Personal Information

Where ARAC no longer requires personal information for any purpose for which the information may be used or disclosed under the Australian Privacy Principles (APP), ARAC must take reasonable steps to destroy the information or to ensure that it is de-identified. This requirement applies except where:

- The personal information is part of a Commonwealth record; or
- ARAC is required by law to retain the personal information.

The disposal of data when it is no longer required is managed in accordance with the following legislation depending on the nature of the information:

- Corporations Act 2001;
- Privacy Act 1988; and/or
- Fair Work Act 2009.