

Privacy Policy

Version 2024.01 | 22 July 2024

Our privacy policy is based on the 12 principles of the Privacy Act and is summarised below.

THIS STATEMENT APPLIES TO ARO ACCOUNTING LTD AND ARO ADVISERS LTD “US”. YOU AGREE THAT YOUR DATA CAN BE SHARED BY THESE TWO ORGANISATIONS.

PRINCIPLE 1 – PURPOSE OF COLLECTION: We will collect information that we need in order to carry out, support and enhance our services which the client has engaged us to do and as we are required to by law.

Information to be collected:

- Full legal name of all entities involved
- Company, partnership or Trust details and legal documents
- IRD number
- Address
- Phone number
- Email address
- Accounting records
- Bank account number
- In some cases where AML applies, ID and source of wealth / funds
- In some cases, details of related parties, such a contact details of beneficiaries

We will use this data to provide the service to you. It will also be used to provide you with support. We will also use the data to enhance our website and services to you.

PRINCIPLE 2 – SOURCE OF INFORMATION: We will get the information directly from the client, except in cases when this may not be possible / convenient - with the consent of the individual concerned.

Other sources:

- Where appropriate, from a holder of the Power of attorney
- Where appropriate, from Parents
- Spouse
- Solicitor

PRINCIPLE 3 – COLLECTION STATEMENT: We will tell the client how the information will be used in a privacy statement which is included in clause 15 of our terms & conditions (prior to signing).

Privacy Act 1993

The Client authorises us or our agent to:

- a. access, collect, retain and use any information about the Client;
 - i. for the purpose of providing agreed financial services including compliance, accounting, tax, advisory services and related services; or
 - ii. for the purpose of marketing products and services to the Client.
- b. disclose information about the Client, whether collected by us from the Client directly or obtained by us from any other source, to any party as directed by the Client, including a disclaimer statement from us.
- c. Where the Client is an individual the authorities under clause 15.1 are authorities or consents for the purposes of the Privacy Act 1993.
- d. The Client shall have the right to request us for a copy of the information about the Client retained by us and the right to request us to correct any incorrect information about the Client held by us.

Providing the information is optional, but we may not be able to carry out the work for you, or it may be inaccurate, unless we have the full information.

PRINCIPLE 4 – MANNER OF COLLECTION: We will obtain the information in a fair manner. We will only ask our client for the information unless our client directs us otherwise. If there are deficiencies in the information provided, we will discuss with our client how these deficiencies can be resolved.

PRINCIPLE 5 – STORAGE & SECURITY: We will keep the information secure.

Measures taken to ensure security:

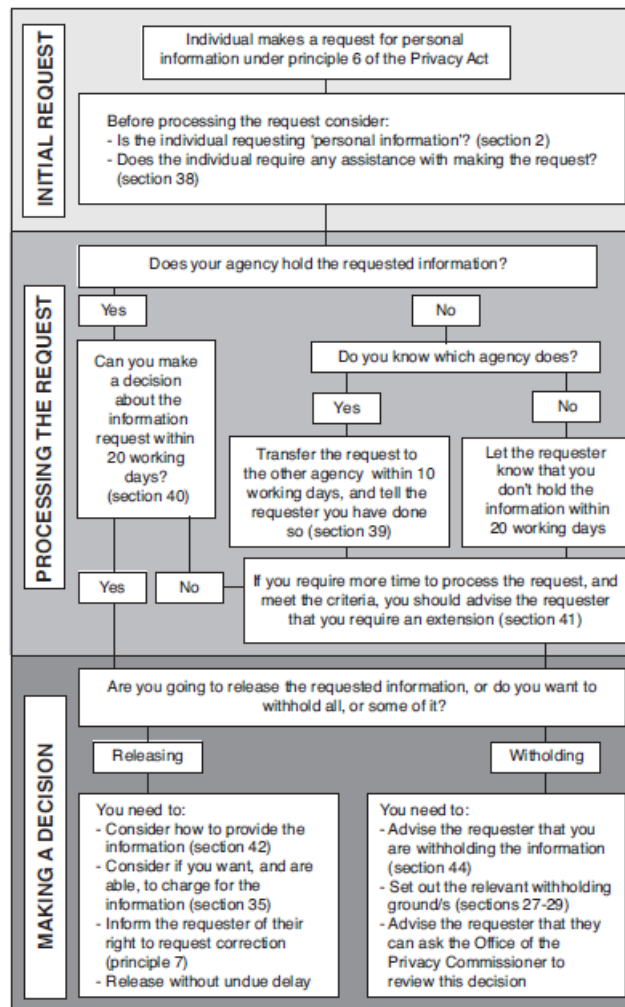
- We use Dashlane and Google authenticator to provide password management and authentication
- We use 2FA with Xero software.

- Recognising that information is stored not only in Sharepoint, but also on local drives in laptops and cell phones, all personnel's computers, tablets and phones require a "key" to get in (key - password, pin, face recognition, fingerprint)
- Devices that are no longer in use, such as laptops, are "cleaned" of client data before they are disposed of.
- We do not use public wi-fi networks if accessing client information, but use a personal hot-spot.
- If we become aware there has been a data breach, our principles are to contain the breach, then evaluate what has occurred, and if the client is at risk then they are to be informed. Measures to prevent a repeat of the breach are to be put in place. See [Plan for Security Incidents and Business Continuity2](#) for more information.
- In case of data breach, we will take the Privacy Office self-assessment to determine if the breach is to be reported to the Privacy Office
<https://privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/evaluate>
- To report a breach, use the Privacy Office's online reporting portal
<https://privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/report-a-breach/>
- Paper records containing IRD numbers and customer details which are no longer needed are either returned to the customer or destroyed.
- The office will be locked when unattended.
- Where we use software to work for you, such as Xero, and we need their support which could involve looking at your private information, we rely on the data privacy undertakings by that organisation.

PRINCIPLE 6 – RIGHT OF ACCESS: Clients have a right to access the information we hold about them.

Follow the chart below:

DEALING WITH A REQUEST FOR PERSONAL INFORMATION



Source: Privacy 101 Workbook participant 17Dec15.pdf, Privacy Commissioner

Reasons we may withhold information:

- May prejudice maintenance of the law, for example, where we report a suspicious transaction for AML purposes
- May endanger the safety of any individual
- May involve the unwarranted disclosure of the affairs of another individual
- Information is confidentially supplied evaluative material
- May prejudice physical or mental health
- Information is not readily retrievable or does not exist or cannot be found

PRINCIPLE 7 – RIGHT OF CORRECTION: Clients have the right to correct information we hold about them.

Because we are often dealing with Government Departments as agents for the individual, we expect that our client will advise us of errors in name, address or other details when we present them with forms to sign when lodging information on their behalf. We will correct that information in our records.

PRINCIPLE 8 – ACCURATE INFORMATION: We are to take care that the information we're using is accurate, complete, relevant and up to date.

Our procedures require the client to confirm details before we lodge information or to check data submitted. Where we are directed to supply information to a third party on behalf of the client, we always provide a copy to our client.

PRINCIPLE 9 – RETENTION OF INFORMATION: We will only keep the information as long as we need it, or we are required to by law – when a client is no longer our customer, we will remove their folder from our clients working folder, and transfer the records to an archive folder. The archive folder are arranged and scheduled for destruction in seven years' time.

- Paper records belonging to the client should be returned to the client or destroyed if directed by the client.
- Electronic files are to be deleted as above
- Where we are the Xero subscriber, we delete the Xero subscription.

PRINCIPLE 10 – USE OF INFORMATION: We will only use the information for the purpose set out in our engagement, or as instructed by the client.

PRINCIPLE 11 – DISCLOSURE OF INFORMATION: We will only disclose this information as per our collection statement or if we have good reason to do so.

Reasons such as:

- Disclosure is necessary to uphold or enforce the law
- Disclosure is necessary for court proceedings
- The person concerned authorised the disclosure

- The information is going to be used in a form that does not identify the person concerned
- Disclosure is necessary to prevent or lessen a serious threat to public health or safety or the life or health of the individual concerned

PRINCIPLE 12 – UNIQUE IDENTIFIERS: We will only use unique identifiers where this is clearly allowed.

The unique identifiers we require are:

- IRD number
- Company Number / NZBN
- In cases of AML, driver licence number / passport number