PRIVACY STATEMENT

Ōtākaro Ltd is committed to protecting confidentiality and the privacy of information entrusted to us.

LAST UPDATED: 30 June 2022

1. Overview

This Privacy Statement explains how Ōtākaro Limited and its agent(s)[1] collect, store, use, disclose and dispose of that personal data. The Statement also outlines how individuals may access, correct and delete information held about them.

Personal information means identifiable information about an individual, such as their name, email, image, address and telephone number etc. Sensitive information means a special category of personal information containing information regarding racial or ethnic origin, political opinions, religious beliefs, genetic data, health information etc.

We will only gather and use personal and sensitive information when it is necessary for us to deliver our services, perform contracts, carry out other necessary business functions and activities, and meet our health and safety, and legal obligations. We will not use or disclose personal information for purposes unrelated to our business activities and the services we provide unless we first obtain an individual's consent.

2. What information do we collect?

Information individuals provide to us directly: We may collect personal information directly from individuals when they provide it in person (such as internally to HR), and/or when they complete any form (including online forms and booking systems). Examples include:

- Contact details: full name; correspondence address; telephone number; email address; banking/credit card information; emergency contacts; details of public social media profile(s).
- Demographic information: gender; date of birth; age; nationality; title; language.
- Consent records: records of any consent individuals may have given and the subject matter of that consent.

Information we get from third parties: We collect or obtain personal information from authorised third parties (e.g. Yellow pages, white pages, industry websites, recruitment agencies, police, external security consultants). Examples of personal information include:

- Contact details: full name; correspondence address; telephone number; email address; details of public social media profile(s).
- Demographic information: gender; date of birth; age; nationality; title; language.

[1] The Privacy Statement applies to all Ōtākaro and its agent(s), including employees; secondees; head office contractors (Ōtākaro staff); general contractors; and consultants (non-staff).

Information we collect automatically: We may automatically collect personal information about individuals when they visit our websites, like an individual's IP address and device type. Some of this information may be collected using cookies and similar tracking technologies. Where cookies are used, a statement will be sent to your browser explaining the use of cookies.

Information we create in the performance of a contract or service: We may also create or obtain personal information, such as evaluation material for recruitment purposes, and from any interactions we have with others on an individual's behalf.

Information individuals make public: We may collect or obtain personal information that individuals manifestly choose to make public, including via online channels such as social media (e.g. LinkedIn, Facebook etc.)

Images we collect through CCTV: We may collect or obtain an individual's image via closed circuit television for health and safety, and security purposes.

Information we collect for investigations: We may collect or obtain an individual's personal information during an internal investigation into Staff misconduct or other security risks to the Company.

A Privacy Impact Assessment will be done prior to an investigation. The Chief Executive will have sole accountability and oversight in matters involving internal staff investigations. Where an investigation involves the unlikely event of surveillance, the Chief Executive will inform the Board.

3. Why do we collect it?

We collect personal information for the following reasons:

- project procurement cycle, such as the selection, management and delivery of project contracts;
- the administration of contractors and subcontractors, including invoicing and payment of invoices;
- land management and divestment;
- administering and planning human resources (including health and safety);
- reporting / disclosing information to Government bodies or other agencies to meet legislative or governance obligations. For example, the Treasury, Department of Prime Minister and Cabinet (DPMC), Inland Revenue, the Ombudsman, Privacy Commissioner etc.;
- stakeholder collaboration, such as sharing project information with key stakeholders;
- IT – user management;
- to protect and improve safety for individuals and reduce the risk of crime and disorder;
- Te Pae operations;
- internal investigations related to Staff misconduct and other security risks to Ōtākaro Limited.

4. How is personal information processed?

Where we collect personal information, we will only process it:

- to perform a contract; or
- to perform a service; or

- where we have legitimate interests to process the personal information or sensitive information and these interests are not overridden by an individual's rights; or
- in accordance with a legal obligation; or
- where we have an individual's consent.

We may use the personal information we have collected for purposes related to the above including:

- to process and administer a contract or service, and to help us develop, improve, manage, administer and facilitate the contract terms and business operations;
- to contract with authorised individuals;
- verify an individual's identity and details;
- for general internal purposes (such as record keeping, database management, training, billing);
- assist with the resolution of any issues relating to a contract;
- to comply with all laws and regulations in all applicable jurisdictions;
- to communicate with the individual; and
- to comply with key Ōtākaro policies.

5. In what limited circumstances might we disclose personal information?

An individual's personal information will not be sold, traded, rented without the individual's consent.

We will only disclose personal information externally if it is necessary and appropriate to facilitate the purpose for which the personal information was collected pursuant to this Privacy Statement, including the carrying out of a contract, service, or a directly related purpose. This may include, for example, disclosing personal information to:

- third party service providers, including any sub-contractors, to enable us to provide services and comply with a contract;
- comply with any court orders, subpoenas or other legal process, or investigation including by government authorities, if such disclosure is required by law. Where possible and appropriate, we will notify the individual if we are required by law to disclose an individual's personal information;
- where disclosure is authorised by the individual concerned;
- avoid prejudice to the maintenance of the law;
- prevent or lessen a serious and imminent threat to public or individual health and/or safety (note that disclosure would be to someone who can do something about it e.g. the Police);
- to a member of Ōtākaro Management or an appropriate third party agency (e.g. Police) where there is an emergency situation requiring a staff member's emergency contact details be released.

In all other situations, where staff need to share an individual's personal data with an external party, staff will first get the individual's written consent (email is acceptable) and keep a note of that consent on record.

If there are parties we routinely share personal data with or transfer large qualities too, we will ensure data sharing agreements are in place. We will review such data sharing agreements regularly.

We will also ensure that appropriate security measures protect data that is in transit, received by us, or transferred externally.

6. International data transfers

When we disclose data, it may be transferred to, and processed in, countries other than New Zealand where our data hosting servers are located. There may be differences with New Zealand's privacy laws. However, where we disclose personal information to a third party in another country, we place safeguards to ensure the personal information is protected.

For individuals in the European Economic Area (EEA), this means their personal information may be transferred outside of the EEA. Where personal information is transferred outside the EEA, it will only be transferred to countries identified as providing adequate protection for EEA data (like New Zealand), or to a third party where we have approved transfer mechanisms in place to protect your personal information (e.g. by entering into the European Commission's Standard Contractual Clauses).

Details of international transfers will be recorded and kept on file as described in the disclosure of personal information section above.

7. Storage and Security

We are committed to protecting the security of individuals personal information and we take all reasonable precautions to protect it from unauthorised access, modification or disclosure.

We implement and maintain security measures designed to provide reasonable protection against the loss, interference or misuse of personal information and to prevent unauthorised access, modification or disclosure of that information.

Personal information stored physically:

- is protected by such security safeguards as it is reasonable in the circumstances including:
    - ensuring personal information is not exposed to unauthorised people; and
    - restricting unsupervised building access to employees only.
- is only accessible from storage when the person accessing the personal information logs their details in a register recording access and return. For records maintained in long-term storage by the contracted provider of secure storage, access logs will be maintained in electronic format. This log will record the personnel members name, business unit, date of request and the date of return.

8. Privacy Breach

A privacy breach occurs when an organisation or individual either intentionally or accidentally:

- Provides unauthorised or accidental access to someone's personal information.

- Discloses, alters, loses or destroys someone's personal information.
- A privacy breach also occurs when someone is unable to access their personal information due to, for example, their account being hacked.

In accordance with the Privacy Act 2020, if a privacy breach has caused or is likely to cause anyone serious harm, we will notify the Privacy Commissioner and any affected people as soon as we are practically able. As a general rule, we will aim to issue a notification within 72 hours.

9. What about links to other websites?

Our websites may contain links to other websites that are not under our control. These websites may use cookies. It is the responsibility of those third parties to collect appropriate consents from individuals to permit their own cookies (to the extent this is required by law) and to inform individuals about the cookies they use. Individuals should check the privacy policy on all third-party websites to ensure they are comfortable with third party cookies.

We have no responsibility for linked websites, and provide them solely for individuals information and convenience. We specifically disclaim responsibility for their content, privacy practices and terms of use, and we make no endorsements, representations or warranties about their accuracy, content or thoroughness. An individual's disclosure of personal information to third party websites is at their own risk.

10. Email, text and telephone communications

We are committed to full compliance with the Unsolicited Electronic Messages Act 2007.

By subscribing to emails and/or text communications, or otherwise providing your email address and/or mobile number, an individual consents to receiving emails and/or texts (as the case may be) that promote and market our products and services, or the products and services of others, from time-to-time.

Individuals can unsubscribe from our email communications and/or text communications at any time by clicking the "Unsubscribe" link in any promotional or marketing email.

Once an individual has unsubscribed from the email or text communications, they will be removed from the corresponding marketing list as soon as is reasonably practicable.

11. Accessing, correcting or deleting personal information

An individual may request access to their personal information, or request we update or correct any personal information we hold about them, or ask us to restrict or cease processing the personal information or even delete personal information.

Individuals should set out their request in writing and send it to us at info@otakaroltd.co.nz review such requests as soon as reasonably practicable to comply with our legal obligations (our target response is

20 working days). If we are unable to grant the individual request, we will give the reasons for this decision in writing.

12. Retention of your Privacy Data

The length of time we keep personal information depends on what it is and whether we have an ongoing business need to retain it (for example, to perform a contract term or to comply with applicable legal requirements such as money laundering and financial reporting legislation).

We retain personal information for as long as we have a relationship with an individual and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our internal retention policies and practices. Following that period, we make sure it is deleted or anonymised. Otherwise, as a general rule, we only keep personal information for as long as we require it for the purposes of performance of the contract or to meet a legal obligation.

13. Privacy Officer

If an individual has any concerns about privacy or the use or collection of personal information by us they can contact our Privacy Officer at info@otakaroltd.co.nz, and include the words 'ATT: THE PRIVACY OFFICER'.

We will respond as quickly as possible (our target response is 20 days), and handle all complaints in a way that is fair and consistent. However, if an individual remains dissatisfied, they can make a formal complaint with Office of the Privacy Commissioner.