

<b>Policy owner</b>	Group Technology Manager
<b>Date of publication (revised)</b>	July 2025
<b>Applicability</b>	Delegat Group Employees

## PURPOSE OF THIS POLICY

Delegat Group Limited ('the Company') is committed to protecting personal information in accordance with the New Zealand Privacy Act 2020 ('the Act'), the Information Privacy Principles and applicable Codes of Practice.

Personal information is any information about an identifiable individual. This policy outlines how the Company, including its service providers, collects, uses, discloses, stores, and protects personal information, and clarifies the responsibilities of the Company, its employees, contractors, and service providers. It also outlines how we use information that we may receive from third parties or gather through our service providers.

How the Company use information will depend on the manner in, and the purpose for, which it is collected. The Company will only collect personal information for lawful business purposes through:

- **Directly from individuals** (e.g. during the recruitment and employment processes)
- **Third parties with consent from the individual concerned** (e.g. referees, government agencies, and service providers).
- **Employment or engagement activities** (e.g. salary data, performance reviews, employment relations matters, usage of company property)

As the Company is headquartered in New Zealand with legal entities operating across the globe, personal information may be transferred internationally, subject to the privacy laws of each respective country in which those entities are operating.

The Company will only disclose personal information to a foreign person or entity if the individual to whom the personal information relates authorises the disclosure to that foreign entity and before doing so has been informed by the Company that the foreign entity may not be required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act; or the Company believes on reasonable grounds that the foreign entity is subject to privacy laws that, overall, provide comparable safeguards to those in the NZ Privacy Act; or disclosure would otherwise be permissible pursuant to the Privacy Act 2020.

However, to the extent that such use does not conflict with local laws, the Company will endeavour to ensure that use of personal information by any Deleat Group entities and third parties is in accordance with this Privacy Policy.

## Examples of Personal Information

Please note that the examples listed are not an exhaustive list but are intended to provide a general idea of the types of information considered as Personal Information.

- Personal details, contact and emergency contact details (e.g. full legal name, preferred name, address, date of birth, email and phone number)
- Employment history, qualifications, references and any other information provided in a CV or in the interview process
- Where relevant, psychometric assessments of abilities and preferred behavioural styles.
- Tax number and code, bank account number, details about superannuation schemes.
- Right to work status, supported by evidence, including verification with a third party (e.g. Immigration).
- Where relevant, Driver licence and credit checks, supported by evidence, including verification with third party (e.g. NZTA).
- Where relevant, criminal history and pending convictions, including verification with a third party (e.g. Ministry of Justice and Police Vetting).
- Where relevant, confirmation of qualifications, including verification with a third party (e.g. training institutes).
- Health and safety-related medical information to assess suitability to carry out the role per legal obligations under workplace health and safety requirements.
- CCTV footage.
- Voluntary diversity and inclusion data for statistical purposes e.g. gender, racial/ethnic origin, date of birth, country of birth and languages spoken.
- Information generated during employment or engagement (e.g. terms of employment/engagement, pay and benefits, leave, training and development, matters related to performance such as performance reviews and feedback, matters related to disciplinary actions, complaints or personal grievances).
- Information from public sources (e.g. social media).

## Review of Personal Information

To meet obligations of lawful business operations, the Company will review activities on company property as and when required. Examples could be to review vehicle log of company vehicle (including those of reasonable personal use), expense claims, activities on work devices, work phone or phone plan, company credit card, and changes to right to work status, driver licence status, convictions, CCTV footage, and other information where relevant.

## Responsibilities regarding the collection, use, disclosure, storage and protection of personal information.

### **The Company is responsible for:**

- Informing individuals what personal information the Company will collect and why (e.g. for pre-employment and employment-related purposes), unless the Company has reasonable grounds to

believe such notification would prejudice the lawful purpose of the collection (e.g. covert surveillance measures).

- Providing clarity on whether providing the information is compulsory or voluntary, and the consequences if compulsory information isn't provided.
- Collecting only the relevant personal information for the purpose/s the information has been collected for (e.g. to determine an individual's suitability for a role), or any other purpose authorised by the individual concerned.
- Providing individuals' rights to access, review, and correct their personal information where legally appropriate (evidence may be required in some circumstances e.g. change of bank account).
- Carrying out due diligence on agents/representatives/third parties to ensure they are aware of and agree to comply with the Privacy Act before engaging with them as authorised agents/representatives/third parties.
- Take reasonable steps to ensure information is reasonably accurate before using it (e.g. unsolicited information), providing the individual of concern an opportunity to provide input and details to explain whether the information is correct or inaccurate.
- Only disclosing information with the consent of the individual concerned (e.g. request by third party or a foreign entity), or where disclosure of the information is one of the purposes in connection for which the information was obtained, or is directly related to the purpose in connection with which the information was obtained, or in circumstances allowed by the Act or any other relevant law governing business operations.
- Keeping personal information safe and secure from loss and/or unauthorised access, use, modification, or disclosure.
- Safely destroying personal information collected when it is no longer required for the purposes for which the information was collected.
- Investigating potential interferences with or breaches of privacy rights.
- Notifying the Company Privacy Officer, affected individuals and/or the New Zealand Privacy Commissioner as soon as practicable after becoming aware of the occurrence of a notifiable privacy breach.

**Employees are responsible for:**

- Ensuring information provided is current, accurate and complete.
- Disclosing all relevant mandatory information about them as part of their pre-employment application or pre-engagement application process to enable the Company to assess their suitability for the role they have applied for or work of interest.
- Disclosing information that may impact the Health and Safety of themselves and others.
- Understanding their rights to access, review, and correct their personal information where legally appropriate (evidence may be required in some circumstances e.g. change of bank account).
- Ensuring the privacy of others with a connection to the Company (including, but not limited to employees, contractors, customers, clients, suppliers, agents, Directors and Shareholders) is protected and is not breached (e.g. through unauthorised/inappropriate access and/or misuse of information).
- Immediately notifying the Company of any involvement in or knowledge of any actual or potential interferences with or breaches of privacy rights.
- Comply with the investigation of potential interferences with or breaches of privacy rights.
- Complying with all other obligations set out in the Privacy Act, local legislations or regulations related to Privacy and/or any other relevant Company policies.
- Notifying the Company Privacy Officer as soon as practicable after becoming aware of the occurrence of a notifiable privacy breach.

**Service Providers and Contractors are responsible for:**

- Ensuring information provided is current, accurate and complete.
- Disclosing all relevant mandatory information about them as part of their pre-employment application or pre-engagement application process to enable the Company to assess their suitability for the role they have applied for or work of interest.
- Disclosing information that may impact the Health and Safety of themselves and others.
- Ensuring the privacy of others with a connection to the Company (including, but not limited to employees, contractors, customers, clients, suppliers, agents, Directors and Shareholders) is protected and is not breached (e.g. through unauthorised/inappropriate access and/or misuse of information).
- Immediately notifying the Company of any involvement in or knowledge of any actual or potential interferences with or breaches of privacy rights.
- Comply with the investigation of potential interferences with or breaches of privacy rights.
- Complying with all other obligations set out in the Privacy Act and local legislations or regulations related to Privacy.
- Notifying the Company Privacy Officer as soon as practicable after becoming aware of the occurrence of a notifiable privacy breach.

## Company Privacy Officer

If you have any questions or comments about this policy, wish to obtain more information about how we manage personal information, or wish to raise concerns, you can contact the Company Privacy Officer:

*Willem van der Steen*

*Group Technology Manager based in Auckland, New Zealand.*

*[willem.vandersteen@delegat.com](mailto:willem.vandersteen@delegat.com)*

*+64 9 359 7300*

## COUNTRY AND/OR REGIONAL VARIANCES OR EXCEPTIONS

This policy has been developed to align with relevant legislation in New Zealand and provides guidance for the Company's global teams. In the event of an inconsistency between the provisions of this policy and those of the Privacy Act and relevant local legislations or regulations, the latter will prevail. The Delegat Privacy Officer can assist you in finding your relevant legislation or regulation if required.

**Group Technology Manager**  
Delegat Limited