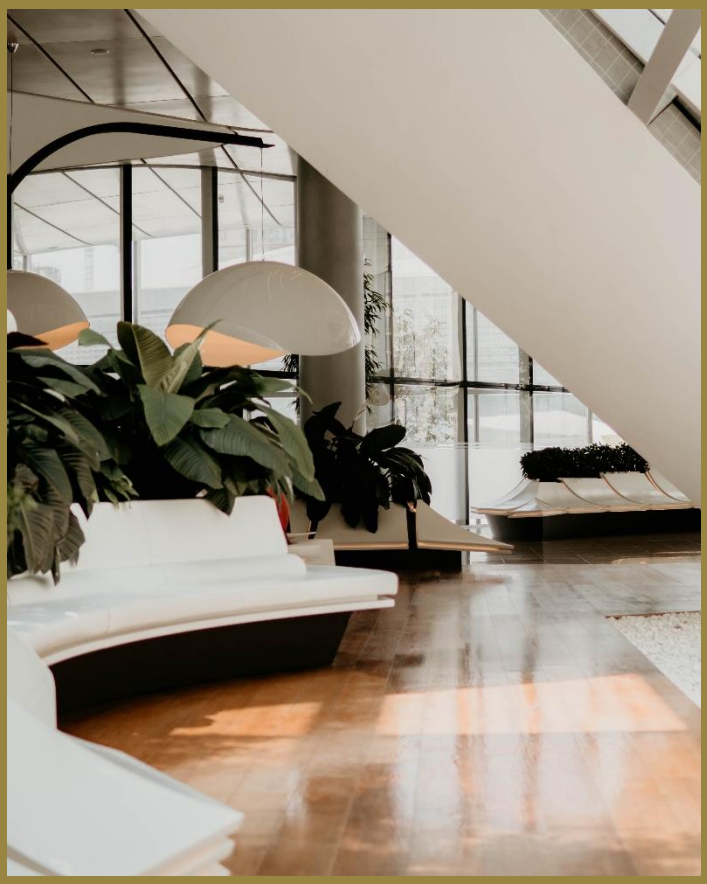
ANZ-POL053-Engaged persons privacy policy

July 2026



Document owner	Legal & Governance
Document author	Legal & Governance
Document number	POL053

Version control

Version	Date	Author	Notes
V.01	03/08/2022	General Counsel/ Chief Risk Officer	Tabled at RCC and approved
V.01	03/08/2022	General Counsel/ Chief Risk Officer	Tabled at RCC and approved

Approval history

Version	Date	Approver	Notes/signature
V 0.3	06/01/2025	General Counsel	Updating personal information references, remove cookies reference, and to bring policy in line with up to date privacy legislation.
V 0.4	01/05/2026	Head of Legal & Governance	Updating where information may be received indirectly in line with up to date privacy legislation.

Engaged persons privacy policy

1 Overview

This Privacy Policy ('Policy') applies to all applicants, current and ex-employees & contingent workers (independent contractors, freelancers, consultants, advisors or other out-sourced workers) ('you', 'your' or 'yours') of DUAL Australia, DUAL New Zealand and their related entities ('we' 'us' or 'our').

This Policy sets out the types of personal information we collect from you and how we will use your personal information.

By applying for or accepting employment or contract work with us you agree to be bound by this Policy and to our collection, use and disclosure of your personal information in accordance with this Policy. If you have any queries about the process, or how we handle your personal information please contact HR or the Legal & Governance team.

2 Changes to this policy

We may change or update this Policy at any time.

We will tell you when we make material changes to this Policy.

3 Categories of data

During your engagement, recruitment, employment and post-employment with us, we may collect and process the following categories of data including, but not limited to:

Categories of data	Employment category
Engagement related data: • Name, address, Date of Birth (DOB), contact information, gender, National Identity details, number, bank details, marital status, driver's license, details of any disabilities which require workplace adjustments, photos, hobbies, interests and diversity data including but not limited to ethnicity, race, religious beliefs and sexual orientation.	• Applicants • Employees • Contingent workers • Ex-employees
Emergency contact details: • Name, relationship to the employee, contact details • Employee personal contact details (for Emergencies)	• Employees • Contingent workers • Ex-employees
Recruitment and selection: • Job history, education - qualification certificates, agency name, referral details, interview notes, tests, pre-employment screening, conflict of interest: information on directorships, interest in other companies, candidate survey feedback and reporting.	• Applicants • Employees • Contingent Workers • Ex-employees
Right to work information: • Passport and visa, National Identity Card or long birth certificate and proof of National Insurance number, proof of address, immigration details, nationality.	• Applicants • Employees • Contingent workers • Ex-employees

Categories of data	Employment category
Employee lifecycle information/changes: • Salary, job details, fit and proper assessment and certificates, Policy period, responsibilities, working hours, location, length of service, working time records, County Court Judgements/Certificate of Earnings, roles in Workday.	• Employees • Contingent Worker • Ex-employees
Reward and benefit data: • Salary, pension, bonus, allowances, shareholding, loans and ad-hoc advances, benefit selections, dependant and beneficiary details including their name, address, DOB and gender, medical information, length of service details.	• Employees • Ex-employees
Family Leave of Absence information: • Parental Leave: Policy of intention to take parental leave, leave balance, leave dates, confirmation of leave, applicable certificates, risk assessments, child's DOB.	• Employees • Ex-employees
Personal and annual leave: • Personal Leave: Doctor's name (or other Medical Practitioner) and address, details of condition, return to work conversation(s), leave dates and reasons, GP/Medical Practitioner report request & response, occupational health referral & response. • Annual Leave: Dates and Leave balance.	• Employees • Ex-employees
Career: • Career development plans, Continuing Personal Development (CPD) data, goals and objectives, development plans, performance, performance rating, talent descriptor, professional institute membership number, professional qualifications, professional qualification sponsorship application(s), Learning Agreement (s).	• Employees • Ex-employees
Employee relations data: • Details of data generated with reference to employee relations policies and processes (which may include but is not limited to Disciplinary Policy, Grievance Policy, Capability Policy/Bullying and Harassment Policy/Whistleblowing Policy or any employment matters where it has been indicated to the employee that a record of the issues will be made). This will include documents such as meetings invitation letters, confirmation of outcome letters, meeting notes/summary notes, personal information referred to during the meeting e.g. Workday records. • Performance improvement emails relating to employee's performance, invitation letters, Performance Improvement Plans (PIP), confirmation of outcome of PIP, confirmation of outcome letters as per Capability Policy and Procedure. • Consultation meeting invites, consultation meeting notes, letter confirming redundancy, settlement agreement and correspondence with legal representatives (if applicable), calculation sheets for redundancy payments, completion of statutory forms e.g. HR1. • Flexible working application (s), flexible working outcome letter, employee file notes.	• Employees • Ex-employees • Contingent worker

Categories of data	Employment category
• TUPE details of any claims or actions brought against the Transferor by the employee within the previous 2 years (e.g. Tribunal claims). • Employee Surveys, feedback and reporting.	
Leaver information: • Resignation letter, settlement/redundancy agreement, exit interviews and surveys, death certificate, reason for leaving and regulatory references.	• Employees • Contingent worker • Ex-employees
Expense claim information: • Expense claims past and present	• Employees • Ex-employees
Travel information: Medical data, biometric data, police checks for visas and any other personal/sensitive information required for travel.	• Employees • Contingent workers • Ex-employees

4 Data collection and use

We collect and use your personal information as reasonably necessary for requirement business functions and activities.

The business functions and activities for which we require your personal information are set out below. By way of summary, these include:

- For the performance of our contract with you
- For compliance with a legal obligation to which we are subject
- To initiate/defend legal claims
- To protect the vital interests of individuals
- For our Legitimate Interests (or those of a third party)
- For emergency contact (Everbridge)
- For Travel bookings

Where we have indicated that the collection and use are necessary for our “Legitimate Interest”, we consider that our “Legitimate Interest” is to ensure fair and effective recruitment of suitable personnel and the effective reward, administration, support, development and management of staff. This is important to ensure that the Company continues to meet its business objectives and goals both in the short and long term; maintains its reputation; and continues to attract and retain high calibre staff. Any additional legitimate interests are set out below.

Activities (Purposes)	This is necessary:
Recruitment and selection of all employees including pre-employment screening	• To take steps at the applicant's request to enter a contract of employment. • For the purpose of the legitimate interests pursued by the Company.

Activities (Purposes)	This is necessary:
On-boarding employees onto Workday and other systems and entering into contracts	• To take steps at the applicant's request to enter a contract of employment. • For compliance with regulatory obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Right to Work checks	• To take steps at the applicant's request to enter a contract of employment. • For the compliance with legal obligations to which the Company is subject.
Providing and administering employee remuneration, benefits, incentive schemes and share schemes	• To perform the contract between you and the Company. • For the purpose of the legitimate interests pursued by the Company.
To support HR administration, maintaining and processing general records necessary to manage the employment of the worker (including making Employment Lifecycle changes)	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Allocating and managing duties and responsibilities for employees	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
To provide access, technical support and maintenance for Workday and other information systems	• To perform the contract between you and the Company. • For the purpose of the legitimate interests pursued by the Company.
Managing and operating performance, employee relations cases, employee surveys/feedback and reporting, management information (including diversity monitoring) and other informal and formal HR processes and making related management decisions	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Managing the training, development, promotion, career of employees and succession planning for the business	• To perform the contract between you and the Company. • For the purpose of the legitimate interests pursued by the Company.
Processing information about absence or medical information in order to support employees to get access to benefits, to return to work or providing additional support as applicable	• For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Complying with reference requests where the Company is named by the individual as a referee	• For the purpose of the legitimate interests pursued by the Company.

Activities (Purposes)	This is necessary:
Complying with reference requests for KYC Directors requests	• For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Disaster Recovery, business continuity, Everbridge	• For the purpose of the legitimate interests pursued by the Company. • To protect the vital interests of individuals • Ensure safety of individuals in emergencies including cyber incidents
Management of Company premises, facilities and Health & Safety	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Complying with employment laws and regulation to which the Company is subject in the conduct of its business	• For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
To enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
To comply with lawful requests by public authorities	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company. The Company considers that it has a legitimate interest in ensuring that it complies with all legal requirements placed on it, whether those are EU obligations or non-EU obligations. The Company wishes to maintain its reputation as a good corporate citizen and to act appropriately in all the countries in which it does business.
Providing and administering employee expenses in order to compensate employees appropriately	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Risk and audit management activity (internal and external) to assess and report on risks/results.	• For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Financial planning and analysis	• For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.
Media subscription services	• For the purpose of the legitimate interests pursued by the Company.

Activities (Purposes)	This is necessary:
IT services, management and administration	• To perform the contract between you and the Company. • For the compliance with legal obligations to which the Company is subject. • For the purpose of the legitimate interests pursued by the Company.

Additional information regarding specific processing of personal information may be notified to you locally or as set out in applicable policies. In particular, additional details of I.T. monitoring, call monitoring and management of confidential information are set out in the Company's Information Security Policies.

5 Special categories of personal information

On occasion, we will collect more 'sensitive' personal information as part of the activities described above. For those Company entities subject to the Privacy Act 1988 (Cth) and/or Privacy Act 2020 NZ, this type of personal information is referred to as "Sensitive Information/Data". This may include information related to your health and, to the extent that you provide it to us, information relating to your race, ethnicity, political opinions, religious or philosophical beliefs, sexual orientation and trade union membership.

Where the collection of Sensitive Information/Data takes place, we also collect and use that information on the following basis:

- The collection and use is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws;
- The collection and use is necessary to protect your vital interests or of another person where you are physically or legally incapable of giving consent (for example in exceptional emergency situations, such as a medical emergency); or
- The collection and use is necessary for the establishment, exercise or defence of legal claims.

This will include the following activities and purposes, although this is not an exhaustive list. In each of the cases set out below, the collection and use is necessary for the purposes of carrying out the obligations and exercising the rights of you or the Company in the field of employment law, social security and social protection law, to the extent permissible under applicable laws.

We will collect Sensitive Information/Data as follows:

- In order to assess and review eligibility to work for the Company;
- To carry out the collection of statistical data subject to local laws, or where required to record such characteristics to comply with equality and diversity requirements of applicable local legislation or to keep the Company's commitment to equal opportunity under review;
- For compliance with employment, health and safety or social security laws. For example, to provide statutory incapacity or maternity benefits, avoid breaching legal duties to you, to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to administer the Company's private medical and long term disability schemes, to make reasonable accommodations or adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard;
- To administer your trade union membership and ensuring that any relevant rights that you may have in connection with any Trade Union membership are complied with, as required to enable us to meet our obligations under employment law; and

- To manage and investigate of any complaint under the Company's grievance policy (or other relevant policies), where such characteristics or information are relevant to the particular complaint, in order to comply with employment law obligations.

6 If we receive your information from someone else (indirect collection)

If we receive your information from another party we will take reasonable steps to let you know we have it, why we have it, who we may share it with, who we are and how to contact us, whether any law authorises the collection, and how you can access or correct your information.

7 Criminal conviction data

Where applicable laws permit us, we many need to collect and use data relating to criminal convictions. This will only be undertaken where we have an applicable legal reason, including your consent. The collection of such data will only be for specific purposes as set out under applicable laws. An example would be for pre-employment screening purposes or for the ongoing 'fit for work' assessments of those staff who hold controlled/regulated functions.

8 Consent

We may seek your consent to certain use and disclosure which is not otherwise justified under one of the above functions set out under headings 4 and 5 above. If consent is required for the use and disclosure in question, it will be sought from you separately to ensure that it is freely given, informed and explicit. Information regarding the relevant use and/or disclosure will be provided to you at the time that consent is requested, along with the impact of not providing any such consent.

9 Data source

We may collect your personal information from various sources, including:

- You;
- Your family members, employer or representative;
- Your manager;
- Pre-employment screening providers;
- Benefit providers;
- Professional Qualification Bodies;
- Government agencies and Courts;
- Previous employers; and
- Regulators (depending upon the type of role).

We do not collect more information than we need to fulfil our necessary functions or activities.

Where we ask you to provide personal information to us on a mandatory basis, we will inform you of this at the time of collection and in the event that particular information is required by the contract or statute this will be specified. Failure to provide any mandatory information will mean that we cannot carry out certain HR processes. For example, if you do not provide us with your bank details, we will not be able to pay you. In some cases, it may mean that we are unable to continue with your employment or engagement as the Company will not have the personal

information we believe to be necessary for the effective and efficient administration and management of our relationship with you.

Apart from personal information relating to you, you may also provide the Company with personal information of third parties, notably your dependents and other family members, for purposes of HR administration and management, including the administration of benefits and to contact your next of kin in an emergency. Before you provide such third party personal information to the Company you must first inform these third parties of any such data which you intend to provide to the Company and of the collection, use and disclosure to be carried out by the Company, as detailed in this Policy.

10 Data retention

The Company endeavours to ensure that personal information are kept as current as possible, and that irrelevant or excessive data are deleted or made anonymous as soon as reasonably practicable.

We retain records containing personal data for the life of your employment or engagement and the following 7 years, unless there is a legal or regulatory obligation to do otherwise. This means that some personal information may be retained for varying time periods in order to comply with legal and regulatory obligations and for other legitimate business reasons.

11 Data sharing

We may disclose your personal information internally on a need-to-know basis to:

- local, regional and global Human Resources, including managers and team members;
- local, regional and executive management responsible for managing or making decisions in connection with your relationship with the Company or when involved in a HR process concerning your relationship with the Company (including, without limitation, staff from Business Risk/Compliance, Legal, Human Resources and Information Security);
- system administrators; and
- where necessary for the performance of specific tasks or system maintenance by staff in the Company teams such as the Finance and IT Department and the Global HR information systems support team.

Certain basic personal information, such as your name, location, job title, contact information, employee number, photo and any published skills and experience profile is also accessible to other employees.

Your personal information is also accessed by third parties, and their associated companies and sub-contractors, whom we work together with for providing us with services, such as administration support, payroll services and the hosting, supporting and maintenance of our HR information systems.

Examples of third parties with whom your data may be shared include:

- Recruitment & Selection providers;
- Company professional advisers including, without limitation, solicitors, accountants, insurers, auditors or others advising the Company in any professional capacity;
- Pre-employment Screening providers;
- Benefit providers;
- Employee Survey providers;
- Tax support providers;
- Global Mobility providers;

- Payroll, Benefit and HR Administration providers (including European/Global HR/Payroll/Benefit providers as applicable); and
- Government and Regulatory agencies.

We also share data externally in some circumstances where you ask us to do so e.g. Employee requested references.

We will ensure any third party we share your personal information with acts in accordance with applicable laws, including with respect to data confidentiality and security, and only processes the data in accordance with the required services.

12 Transfer of personal information

As stated above, from time to time your personal information (including Sensitive Information/Data) will be transferred to associated companies of the Company to process for the purposes described in this Policy. These associated companies may be located anywhere in the world. Personal information may also be transferred to third parties (e.g. service providers or regulators as set out above), who may have systems or suppliers located across the globe. In particular, your personal information will be shared with Workday, who provide the Group's HR database, where the personal information will be transferred to/accessed from the US and India, in connection with HR administration processes..

Where this occurs, we will ensure that all appropriate safeguards are in place to protect your personal information, and that transfer is in compliance with applicable privacy laws. We will ensure that service providers (including other Company associated companies) sign appropriate contractual clauses, and any additional obligations as required under the laws of the exporting entity. You can obtain a copy of any of the contractual clauses, relating to the transfer of your personal information by contacting your HR representative. Where your personal information is transferred outside Australia or New Zealand to a recipient not regulated by laws that protect your information in a way similar to the legal requirements of Australia and New Zealand, we will seek your consent to disclose your information, noting that your information may not be given the same protection as provided by the privacy regime in Australia and New Zealand.

13 Your rights

Your personal information rights, set out below, are those that apply where your employing entity, or other party who has your personal information, is based in Australia or New Zealand. These rights are also likely to apply in many other jurisdictions around the globe, but not necessary all of them, and are subject to certain exemptions.

- Right to access and request correction of your Personal Information - We aim to ensure that all personal information is correct. You also have a responsibility to ensure that changes in your personal information are notified to us so that we can ensure that your data is up-to-date. You can see and update most of this data yourself via Workday, or by contacting your HR representative.
    - Subject to certain exemptions, you may have the right to request access to any of your personal information that we may hold, and to request correction of any inaccurate data relating to you. Furthermore, you have the right to request deletion of any irrelevant data we hold about you.
- Data portability - Where we are relying upon the fact that the collection and use of your information is necessary for the performance of a contract to which you are party as the legal basis for that collection, and that personal information is processed by automatic means, you may have the right to receive all such personal information which you have

provided to us in a structured, commonly used and machine-readable format, and also to require us to transmit it to another entity where this is technically feasible.

- Limits of use-

our right to hold and use your personal information is limited to use in connection with the purpose it was collected, unless we believe on reasonable grounds:

  - the information is used in a form where you are not identifiable;
  - the information is used for statistical or research purposes, not to be published in a form that could reasonably be expected to identify you;
  - the purpose for the use has been authorised by you;
  - we have obtained the information from publicly available publications, and it would not be unfair or unreasonable in the circumstances to use that information for another purpose;
  - the use of the information for the other purposes is necessary to avoid prejudice to the maintenance of law by a public agency, for the enforcement of a law, or for legal proceedings before a court or tribunal;
  - the use of the information for the other purpose is necessary to prevent or lessen serious threat to public health or safety, or life or health of an individual.

Where your personal information is subjected to a restriction in this way, we will only process it with your consent or for the establishment, exercise or defence of legal claims.

- Right to object to use of personal information - You may have the right to object to how your personal information is used. If you object, we must stop that use unless we can either demonstrate compelling legitimate grounds, including your consent for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims.
- Right to withdraw consent - Where we have relied on your consent to collect and use your personal information, you have the right to withdraw such consent at any time. However, dependent upon the type of personal information and the reason we are using it, this could have an impact on your role and on your employment.
- Right not to be subject to a decision based on automated processing - Where a legal decision has been made about you that has involved solely automated processing, including profiling, you have the right for this decision to be reviewed.
- Right to complain to the relevant authority - Where you have complained to us in relation to a data protection related matter, and are not satisfied with the outcome, or if you think that we have breached any privacy laws, you may have the right to refer your complaint to the relevant government or regulatory authority. The relevant authorities for Australia and New Zealand are listed below.

Australia	**New Zealand**
Office of the Privacy Commissioner Director of FOI Dispute Resolution, GPO Box 5218, Sydney NSW 2001	Office of the Privacy Commissioner PO Box 10 094, Wellington 6143
Tel: 1300 363 992	Tel: 0800 803 909

Australia	New Zealand
Email: foidr@oaic.gov.au	Website: https://privacy.org.nz/your-rights/making-a-complaint/

14 Queries

We try to meet the highest standards when collecting and using your personal information. If you have a query, want to exercise any of your rights or want to make a complaint about the way we have collected or used your personal information, please contact your HR representative or the Legal & Governance team at compliance@dualasiapacific.com



Helping you do more

Australia | New Zealand
Part of the DUAL International Group

dualinsurance.com