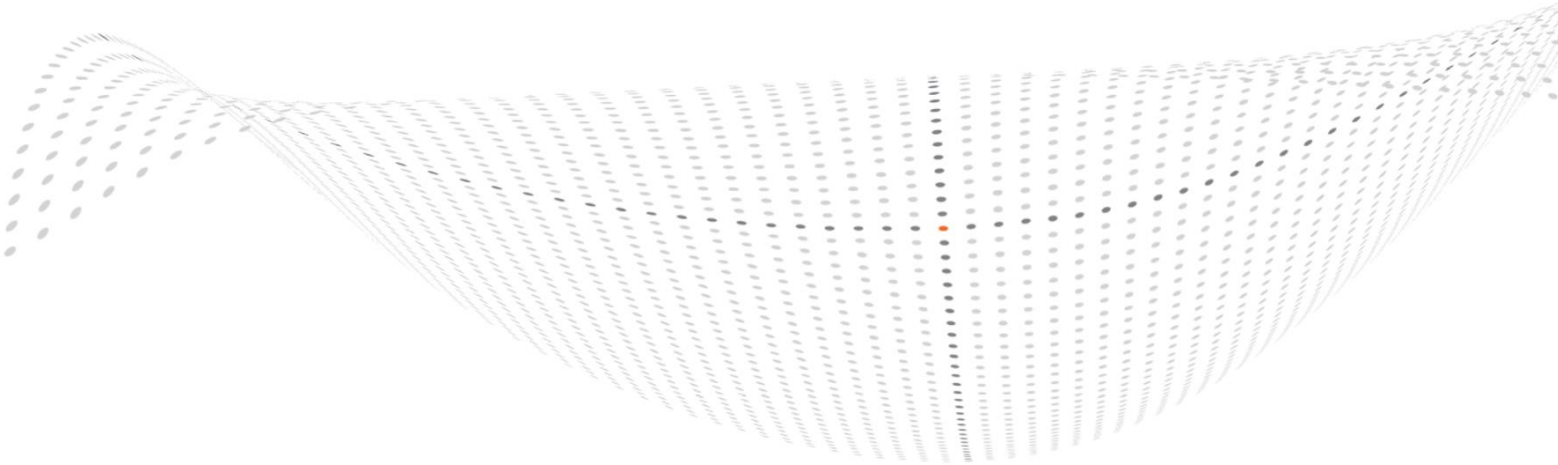
Privacy Policy

Incorporating the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*

For all subsidiaries of the Link Group in connection with Australia

Public Version
Date: 24 February 2016



Contents

The Link Group may make changes to this Privacy Policy from time to time, without notice. This policy was current when last reviewed on 24 February 2016.

1. Introduction

In the conduct of its businesses, Link Group necessarily seeks, records, uses and discloses personal information about individuals.

Link Group entities in connection with Australia are therefore subject to The *Privacy Act 1988* (Cth) (Privacy Act) which regulates how personal information is handled. The Privacy Act defines personal information as:

> ...information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[1]

Quite apart from the law, appropriate management and protection of personal information is important for the safety and security of the individual to whom the information belongs, and for the commercial interests of Link Group.

Link Group is committed to meeting its compliance obligations and protecting personal information. This document explains how we manage personal information, including our obligations and the rights of individuals.

2. Purpose

The purpose of this policy is to record Top Management's commitment and expectation of how personal information is to be handled.

This policy does not detail actual processes, practices, procedures and systems adopted. Rather it sets out the commitment and general principles which are to be interpreted and applied in the conduct of the Link Group's business, as the standing, overriding directive from Management.

3. Scope

This policy applies to any and all persons, corporate or natural, whether employed, contracted or otherwise associated with Link Group and/or its subsidiaries. This is not a stand-alone document. It is supported by the Risk Management and Compliance frameworks, including operational policies, procedures and processes.

Third party service providers may give effect to their own Privacy Policy's, but in any event, must act in compliance with the Privacy Act at all times.

This document has been written to accommodate the changes to the Privacy Act, introduced via the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

1 Section 6 of the Privacy Act 1988 (Cth)

4. Kinds of Information Collected and Held

In the valid discharge of its functions, Link Group usually collects and holds the following kinds of information:

4.1 Personal Information

- Names;
- Date of birth;
- Marital status*;
- Information related to foreign tax status*
- Contact details;
- Employment history*;
- Salary details*;
- Banking details*;
- Beneficiary details*.

* Only if (and insofar as is) relevant and necessary for the provision of contracted or requested services.

4.2 Sensitive Information

Less commonly, but where necessary for the provision of a service or compliance with lawful authority, Link Group may also collect sensitive information including:

- Health information (including physical or mental illness or injury);
- Biometric information;
- Immigration Status;
- Tax file number (TFN) and taxation records;
- Membership of a trade association and/or trade union;
- Details published in Politically Exposed Person (PEP) lists, criminal watch lists, United Nations Sanctions lists and Department of Foreign Affairs and Trade lists (for Anti-money Laundering Counter-Terrorism Financing and Autonomous Sanctions purposes).

5. Australian Privacy Principles (APPs) Addressed

Critical to the Privacy Act are the thirteen APPs,[2] which set out the guiding principles that organisations must take reasonably practicable steps to give effect to, in order to comply. Link Group's response to the APPs are as follows:

5.1 APP 1: Open and Transparent Management of Personal Information

At all times, this policy must:

- Be up-to-date;
- Clearly express how Link Group manages personal information;

2 Formerly, the National Privacy Principles (NPP's) and Information Privacy Principles (IPP's).

- Be made publicly available and free of charge; and
- Be provided in any reasonably requested medium.

Link Group will take reasonable steps to implement practices, procedures and systems to deal with inquiries or complaints from individuals and ensure compliance with the Privacy Act.

5.2 APP 2: Anonymity and Pseudonymity

Link Group will generally enable individuals to remain anonymous (nameless), or to use a pseudonym (fictitious name), wherever it is reasonably practicable to do so.

That is, Link Group will not generally refuse to deal with individuals who do not disclose their identity and will not insist on seeking personal information unless it is lawfully required and/or necessary to provide the contracted or requested service.

An example of an exception is where an individual requests a quote of their financial entitlement, Link Group will need to obtain that individual's personal information in order to locate the record of entitlement and will need to verify the identity of the requestor, before a personalised quote can be lawfully disclosed.

5.3 APP 3: Collection of Solicited Personal Information

The purposes for which Link Group collects, holds, uses and discloses personal information are to provide financial products and services to individuals and wholesale clients, or to validly discharge contractual legal obligations in the provision of administrative or value add services to companies and other product and service providers. If personal information is not collected and recorded, Link Group may not be able to provide services or administer benefits and there could be other consequences such as additional taxation, transfer of entitlements to ASIC, the ATO or to state revenue.

Link Group's usual approach to collecting personal information is, wherever possible, to collect information directly from the individual. Where this is not practicable, information may be collected by lawful and fair means from secondary sources such as from Government agencies, other service providers, publically available sources, employers or from list purchases. Sensitive information about a person will only be collected with the consent of the individual, except where we are required or permitted by lawful authority to collect sensitive information without consent.

Websites of Link Group will collect information using a combination of persistent and non-persistent (session) cookies. Changing browser settings to disable cookies may prevent access to the secured pages within the websites. Browser information collected through the use of cookies is not disclosed to any third party, except where permitted or required by law.

Personal information is usually held in various mediums such as physical documents, soft copy images of documents (in electronic form), electronic data files, records within databases (proprietary and outsourced), telephone call recordings and backup tapes/archive, which are protected by the Link Groups Information Security Management System.

5.4 APP 4: Dealing with Unsolicited Personal Information

Generally, information received by Link Group is immediately and automatically recorded (i.e. all telephone calls are electronically recorded and all documentation received is scanned into an electronic image). This is necessary because Link Group is a trusted third party record keeper, providing technical, administrative, support and/or financial services, involving day-to-day money and security asset movements where imprecise record keeping may have significant adverse consequences.

Where it becomes apparent that a communication contains unsolicited personal information that would not otherwise be lawfully capable of being requested or used under APP 3, Link Group will make reasonable efforts to delete, destroy or de-identify the record.

Where it is impracticable to delete, destroy or de-identify (for example, where the unsolicited information is combined with necessary information) the record will be retained. Reasonable steps are taken to protect the personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse.

5.5 APP 5: Notification of the Collection of Personal Information

More often than not, Link Group acts as agent for its clients. At the point of collecting personal information, individuals will receive, or have access to, a personal information collection notice either from Link Group, or from the primary product or service provider on whose behalf Link Group is acting. Generally, where personal information is recorded, a confirmation communication is provided to the individual.

5.6 APP 6: Use and Disclosure of Personal Information

Personal information held by Link Group will only be used or disclosed for purposes directly related to one or more legitimate functions or activities of Link Group in the provision of its services or as otherwise permitted by lawful authority. Link Group does not sell personal information.

Link Group may permit third parties to access personal information, or may disclose personal information to third parties, in the following circumstances:

- With consent from the individual;
- Where a person would reasonably expect the disclosure;
- Where we have previously notified a person about the use or disclosure;
- Where a permitted general situation is met under the Privacy Act 1988;
- As otherwise permitted or required by lawful authority.

Subject to the law, the people or entities that Link Group may allow to use personal information or may disclose personal information to, include but may not be limited to:

- Link Group staff, contractors, advisers, consultants, analysts, related bodies corporate and auditors;
- For relevant interest and securities holders, the companies and managed investment schemes and other entities whose registers Link Group maintains;
- Employers (in limited circumstances for superannuation purposes and/or employee share plan arrangements (if applicable));
- Law enforcement agencies (State and Federal Police, ASIC etc);
- Government regulators (ATO, AUSTRAC, ASIC, APRA, DHS, Centrelink etc);
- The Australian Securities Exchange (ASX) or other securities exchanges in Australia or overseas where required by lawful authority;
- Superannuation providers (for superannuation administration purposes);
- Identity verification service providers;
- Securities Brokers (If applicable – for share registry services);

Link Group takes all reasonable steps to ensure that the third parties we deal with are bound by confidentiality and privacy responsibilities. Please also refer to APP 8 (Cross Border Disclosure of Personal Information) below.

5.7 APP 7: Direct Marketing

Link Group may provide marketing services on its own behalf and/or on behalf of clients (under contract). Personal information of individuals is only used to market relevant products and services specifically to that individual.

This will only occur with the individuals consent or as otherwise lawfully permitted. Link Group complies with the SPAM Act 2003 and the Do Not Call Register Act 2006.

An individual can opt out of direct marketing at any time by notifying Link Group of the desire to unsubscribe. Such requests can be made electronically (via online accounts or email), in writing by post or by telephone call. Each marketing communication sent by Link Group will contain the details of the opt-out option, which will be promptly honoured.

5.8 APP 8: Cross Border Disclosure of Personal Information

Link Group generally will not send personal information overseas.

However, Link Group is a multinational conglomerate and deals with some overseas third parties. In rare circumstances and under strict control, Link Group may authorise access to personal information by restricted persons in an overseas location. Such countries might include, but are not limited to New Zealand, the United Kingdom, France, Germany, Luxembourg, Switzerland, the United States of America, Papua New Guinea, China [Hong Kong], India, United Arab Emirates, South Africa, Canada and the Philippines.

All entities that Link Group deals with, whether Australian or otherwise, are subject to this or a commensurate policy and commitment to protect personal information.

Some Link Group entities are located overseas. In accordance with its obligations under European law, certain related bodies within Link Group have entered into an 'Intra-Group Data Transfer Agreement', which sets out the minimum standards and obligations of each party when information is handled within Link Group.

5.9 APP 9: Adoption, Use or Disclosure of Government Related Identifiers

Link Group may request, record and use government identifiers for legitimate purposes in the conduct of its business as permitted by law.

For example, an individual's tax file number may be sought, recorded and used to validly discharge taxation obligations. However, government identifiers will not be adopted as Link Group's own identifier.

5.10 APP 10: Quality of Personal Information

Link Group will take reasonable steps to ensure that the personal information we collect, use or disclose is accurate, up-to-date, complete and relevant. Where the personal information held is redundant or misleading, reasonable steps will be taken to correct the information. This may be achieved by re-collecting information directly from the individual and/or independently verifying personal information as required and/or permitted by lawful authority. Refer also to APP 13.

5.11 APP 11: Security of Personal Information

Link Group's information Security Management System utilises various security methods and controls to protect information during the data lifecycle. Such measures include, but are not limited to, masking or scrambling of data in test environments, firewalls, anti-virus, system security patch management, secure identity access management, user access restrictions/ role-based permissions, data encryption, penetration testing, vulnerability assessments, segregated restricted access facilities and staff awareness training.

When personal information is no longer required, reasonably practicable steps are taken to destroy or de-identify the information. Where it is not practicable to do so, reasonable steps are taken to protect the personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse.

Link Group maintains a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. To reassure customers and clients that international best practice recommendations have been followed, Link Group maintains certification against ISO 27001 Information Security Management.

5.12 APP 12: Access to Personal Information

Individuals have a right to request access to their personal information (some restrictions may apply). Such a request may be made verbally and/or in writing. Where such a request is reasonable, access will not be unreasonably withheld.

Access may include a report, transcript, reproduced copy, or right of access to Link Group premises to inspect personal information held. A charge equal to the reasonable cost to reproduce or make copies of personal information may be levied on the requestor.

To lawfully gain access to personal information, Link Group will need to satisfy itself of the identity of the requestor and that the personal information being sought is that of the requestor and not any other individual (including familial relations without relevant authority).

Where a written request to access information is refused, a written notice will generally be issued setting out the reasons for the refusal.

5.13 APP 13: Correction of Personal Information

Individuals have a right to correct personal information held about them. Such a request may be made verbally and/or in writing. In some cases, Link Group may require evidence in support of the requested change to ensure the integrity of the information.

Valid requests to correct personal information will be completed within a reasonable timeframe. If Link Group refuses a written request to update an individual's personal information, a written notice will generally be issued, setting out the reasons for the refusal.

6. Enquiries and Complaints

Link Group has an established internal dispute resolution system in place to efficiently manage enquiries and complaints. Individuals wishing to make enquiries or lodge a complaint in relation to how Link Group handles personal information are encouraged to do so. At first instance, this should be to Link Group directly, via:

Telephone: + 61 1800 502 355 (free call within Australia)
9am–5pm (Sydney time), Monday to Friday (excluding public holidays).

Or in writing, addressed to the Privacy Officer at:

Email: privacy.officer@linkgroup.com; or
Post: Attn: Privacy Officer
Link Group
Locked Bag A14
Sydney South NSW 1235

After exhausting the above, if Link Group is unable to resolve a complaint to the satisfaction of the individual, he or she may be able to refer the matter to the Office of the Australian Information Commissioner (www.oaic.gov.au) who can be contacted by phoning 1300 363 992 or emailing enquiries@oaic.gov.au