

LOCAL GOVERNMENT INFRASTRUCTURE SERVICES PTY LTD PRIVACY PLAN

The *Privacy Act 1988* (Cth) (Privacy Act) applies to small business operators with an annual turnover of \$3 million or more. Local Government Infrastructure Services Pty Ltd (LGIS), as a small business operator with an annual turnover of more than \$3 million, is subject to the Privacy Act.

LGIS is committed to observing the 10 National Privacy Principles (NPPs) set out in schedule 3 to the Privacy Act. LGIS will make this Privacy Plan available to you upon request.

1 What is LGIS?

LGIS is a joint initiative of the Local Government Association of Queensland Inc and Queensland Treasury Corporation.

The key service objective of LGIS is to offer its customers low cost access to the benefits of scale and centralised core competencies in order to reduce the costs and risks of infrastructure procurement by Queensland local government.

LGIS provides services directly or through contracted service providers. Where services are provided through a contracted service provider, LGIS ensures that its privacy obligations are met through appropriate clauses in its contracts with service providers.

At the date of this plan, LGIS has no employees. QTC provides most of the accounting and company secretarial services required by LGIS that information arising from these functions is accessible to QTC staff.

This Privacy Plan has regard to the Privacy Act and the 10 NPPs. The NPPs and certain sections of the Privacy Act are extracted in the appendix.

In practical terms LGIS compliance with the NPPs means that it will:

- not collect personal information unless it is needed for LGIS activities and it is collected in a fair way
- tell persons from whom personal information is collected why it is collected, how it will be used and how they can access and correct it in certain circumstances
- not use personal information for another purpose without consent (unless the exceptions in NPP 2 apply)
- keep personal information safe and up to date and
- delete or destroy personal information when no longer required for the purpose of collection

2 Scope of Personal Information

Personal information is defined as information or an opinion (including that which forms 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.

However, where LGIS retains employee records, they are exempt from the NPPs under s 7B Privacy Act.

3 What Personal Information does LGIS collect, store and use?

3.1 Contractors, secondees and external service providers

LGIS collects personal information about contractors, secondees and external service providers who are individuals (or their principals or employees where they are not individuals). This information is collected and used to select, manage, monitor and pay contractors, secondees or consultants. It is also used to manage conflicts between personal interests and performance of duties. The information may include:

- name and address
- licences or certificates of qualification
- personal interests, directorships, moral rights or other interests
- contact details
- experience and qualifications
- authorised signatory lists
- bank account details
- assessments and opinions regarding performance, and
- Australian Business Number.

3.2 Directors of LGIS

LGIS collects and keeps information about the directors of LGIS for the purposes of taking out, renewing or administering its Directors and Officers Insurance policies, preparing annual reports and returns, administering remuneration (if any) to directors, providing administrative assistance and managing conflicts of interests with director's duties. The information collected may include:

- names
- contact details
- date of birth
- details of other directorships, personal interests and moral rights held
- bank account details
- tax file number, and
- superannuation and employment elections.

Some of this information may be included in the annual reports and returns of LGIS or of the relevant entity where this is required by law, accounting standards or standard business practice.

3.3 Customers and their employees/officers, Suppliers

LGIS collects personal information about its customers, their employees, their office holders and sometimes customers of theirs, where LGIS is supplying to those customers. The information collected by LGIS may include:

- qualifications and education
- work history
- position within an organisation
- levels of authorisation
- signature
- attendance at LGIS-sponsored seminars/conferences
- personal interests and family

- address
- gifts and hospitality given and received, and
- complaints or feedback about services provided.

This information is used for day to day work contact and management of services for the customers, to provide information to individuals about other services provided by LGIS, to investigate complaints or to organise general marketing and client relationship activities with the individuals concerned.

When LGIS contracts to purchase goods or services, it collects and keeps information about other parties to the contracts for contract management and administrative purposes. The information collected may include:

- names
- contact details

3.4 Cookies and emails

The LGIS web site may use cookies to provide better services or measure internet access to its site. You may be asked to accept cookies, in which case your internet address will be recorded. This record will be used only as a measure of site access.

Any e-mail correspondence sent to our organisation may be monitored; however, we will not disclose your details to a third party without your consent unless required by law or an exception in NPP 2 applies.

4 Disclosure and Availability

Personal information that is kept by LGIS is generally accessible to QTC staff performing company secretarial or accounting services for LGIS, all LGIS staff and Directors. From time to time LGIS may need to disclose some types of personal information to other organisations or individuals outside LGIS. Examples of external disclosures include disclosures of:

- personal information reasonably required for LGIS to perform its functions, or required by law
- tax file numbers and Australian Business Numbers to taxation authorities, and
- filing statutory returns and notices to the Australian Securities and Investments Commission under the *Corporations Act 2001* and publication of information about directors in annual reports.

5 Retention

LGIS may keep its records in electronic or hard copy form (or both) and destroys them in accordance with the requirements of the Public Records Act 2002 (Qld). Personal information within records is redacted when no longer needed for the purpose for which it was collected.

6 Access by individuals to their Personal Information

LGIS provides for access to, and correction of, records of personal information kept about individuals, except where the exceptions in NPP 6 apply. These exceptions generally relate to

when access might infringe the privacy of another person, might prejudice a court case or an official investigation or might pose a threat to a person.

7 Steps to take to access or correct your Personal Information

If you wish to access your personal information, or are concerned that it needs correction, contact the Privacy Officer. LGIS may require you to verify your identity and/or to provide a written request for personal information or the reasons it needs to be corrected, so that it can reasonably identify the information.

LGIS will endeavour to respond to your application as soon as reasonably possible. In any event, LGIS shall respond not later than 14 days after receiving the request in writing.

The contact details of the Privacy Officer are:

Address: Privacy Officer
c/o Queensland Treasury Corporation
GPO Box 1096
Brisbane Qld 4001

Email: privacyofficer@qtc.com.au
Phone: 07 3842 4739
Facsimile: 07 3236 9031

8 Use of Personal Information

LGIS will not use or disclose personal information to anyone other than the individual concerned unless, in terms of NPP 2:

- (a) the individual concerned is reasonably likely to have understood, or have been made aware, at the time of collection that information of that kind is used as proposed, **it is not practical to obtain consent for a marketing use and the individual is given the opportunity to “opt out”, at no cost**
- (b) the individual concerned has consented to the proposed use or disclosure
- (c) the proposed use or disclosure is required or authorised by law
- (d) the proposed use or disclosure is reasonably necessary to prevent or lessen a serious and imminent threat to a person’s life or health, or
- (e) the proposed use or disclosure is reasonably necessary for enforcement of a criminal law or a law imposing a pecuniary penalty or for protection of the public revenue.

9 Resolving your concerns

If you have any questions, concerns or complaints about your privacy, please raise them with the person you usually deal with at LGIS, or the relevant program call centre that has been established, or the Privacy Officer. LGIS may ask you to put your concern in writing.

LGIS has a policy dealing with how LGIS resolves complaints. The policy is accessible through LGIS webpage and is also available upon request.

Appendix: PRIVACY ACT 1988

s 7 Acts and practices of agencies, organisations etc.

- (1) Except so far as the contrary intention appears, a reference in this Act (other than section 8) to an act or to a practice is a reference to:
 - (a) an act done, or a practice engaged in, as the case may be, by an agency (other than an eligible case manager or an eligible hearing service provider), a file number recipient, a credit reporting agency or a credit provider other than:
 - (ee) an act done, or a practice engaged in, by an organisation, other than an exempt act or exempt practice (see sections 7B and 7C);

s 7B Exempt acts and exempt practices of organisations

- (3) An act done, or practice engaged in, by an organisation that is or was an employer of an individual, is *exempt* for the purposes of paragraph 7(1)(ee) if the act or practice is directly related to:
 - (a) a current or former employment relationship between the employer and the individual; and
 - (b) an employee record held by the organisation and relating to the individual.

Schedule 3 : National Privacy Principles

1. Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
 - (a) the identity of the organisation and how to contact it; and
 - (b) the fact that he or she is able to gain access to the information; and
 - (c) the purposes for which the information is collected; and
 - (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
 - (e) any law that requires the particular information to be collected; and

- (f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2. Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the *secondary purpose*) other than the primary purpose of collection unless:

(a) both of the following apply:

- (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
- (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

- (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
- (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
- (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
- (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
- (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
 - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- (e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
 - (i) a serious and imminent threat to an individual's life, health or safety; or
 - (ii) a serious threat to public health or public safety; or
- (ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:
 - (i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; or
- (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (g) the use or disclosure is required or authorised by or under law; or
- (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

- (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
- (iii) the protection of the public revenue;
- (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
- (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisations primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) **the individual:**

- (i) is physically or legally incapable of giving consent to the disclosure; or
- (ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the *carer*) providing the health service for the organisation is satisfied that either:

- (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
- (ii) the disclosure is made for compassionate reasons; and

(c) **the disclosure is not contrary to any wish:**

- (i) expressed by the individual before the individual became unable to give or communicate consent; and
 - (ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and
- (d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is **responsible** for an individual if the person is:

- (a) a parent of the individual; or
- (b) a child or sibling of the individual and at least 18 years old; or
- (c) a spouse or de facto spouse of the individual; or
- (d) a relative of the individual, at least 18 years old and a member of the individual's household; or
- (e) a guardian of the individual; or
- (f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
- (g) a person who has an intimate personal relationship with the individual; or
- (h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3. Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4. Data security

- 4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- 4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5. Openness

- 5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.
- 5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6. Access and correction

- 6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:
 - (a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or
 - (b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or
 - (c) providing access would have an unreasonable impact upon the privacy of other individuals; or
 - (d) the request for access is frivolous or vexatious; or
 - (e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
 - (f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
 - (g) providing access would be unlawful; or
 - (h) denying access is required or authorised by or under law; or

- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
- (j) providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

- (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

- (a) must not be excessive; and
- (b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

- 6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.
- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7. Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

- (a) an agency; or
- (b) an agent of an agency acting in its capacity as agent; or
- (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
- (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
- (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an ***identifier***.

8. Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9. Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or
- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10. Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

- (a) the individual has consented; or
- (b) the collection is required by law; or
- (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

- (i) is physically or legally incapable of giving consent to the collection; or
- (ii) physically cannot communicate consent to the collection; or
- (d) if the information is collected in the course of the activities of a non-profit organisation the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
- (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

- (a) the information is necessary to provide a health service to the individual; and
- (b) the information is collected:
 - (i) as required or authorised by or under law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

- (a) the collection is necessary for any of the following purposes:
 - (i) research relevant to public health or public safety;
 - (ii) the compilation or analysis of statistics relevant to public health or public safety;
 - (iii) the management, funding or monitoring of a health service; and
- (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - (i) as required by law (other than this Act); or

- (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;
or
- (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.