Tasmania

*Electricity Supply Industry Act 1995*

*Electricity Supply Industry (Customer) Regulations 2012*

*Electricity Supply Industry Distribution Licence – Aurora Energy Pty Ltd*

*Electricity Supply Industry (Network Performance Requirements) Regulations 2007 (TAS)*

*Electricity Supply Industry (Price Control and Related Matters) Regulations 2012 (TAS)*

*Electricity Supply Industry Regulations 2008 (TAS)*

Victoria

*Electricity Customer Metering Code 2012 (Vic)*

*Electricity Distribution Code 2012 (Vic)*

*Energy Retail Code 2012 (Vic)*

*ACTEW Retail Limited, AGH ACT Retail Investments Pty Ltd Trading as ACTEWAGL Retail Electricity Retail Licence* as varied on 31 July 2002

*SPI Electricity Pty Ltd Electricity Distribution Licence* as varied 14 January 2005

By way of example, Appendix D includes a review of specific licences. In jurisdictions where there is more than one relevant licensee, an assumption is made that the identified provisions are uniform across all licences. This seems reasonable given the nature of the obligations which are general rather than specific to the particular licensee.

Western Australia

*Code of Conduct for the Supply of Electricity to Small Use Customers (Electricity)* – Part 10

*Electricity Industry (Metering) Code* *2012* – Clause 5.17A and Part 7

*Electricity Industry Customer Transfer Code 2004* (contestable customers only) – Part 3

*Electricity Industry (Customer Contracts) Regulations* *2005* – Regulation 19

*Electricity Industry (Wholesale Electricity Market) Regulations* (the *WEM Rules*)

*Energy Coordination Act* *1994* – Part 4

## Government and regulatory reports and papers

Essential Services Commission Victoria, *Smart Meter Privacy Impact Assessment*, Draft Report, May 2012

Ministerial Council on Energy Standing Committee of Officials, *Smart Meter Customer Protection and Safety Review – Draft Policy Paper One*, August 2009

Standing Council on Energy and Resources, *Statement on smart meters for small customers: future directions*, 8 June 2012

Standing Council on Energy and Resources Senior Committee of Officials’ Energy Market Reform Working Group, *National Smart Meter Consumer Protection and Safety Review*, Officials’ Report, November 2012

Public Record Office Victoria, *Use of Back-up Technology to Archive: Issues Paper,* 2012

## Consultant reports

Deloitte, *Advanced metering infrastructure cost benefit analysis*, prepared for Victorian Department of Treasury and Finance, Final report, 2 August 2011

Futura Consulting, *Advanced Metering Infrastructure Program – Benefits Realisation Roadmap*, prepared for Victorian Department of Primary Industries, Final Report, 10 December 2009

Lockstep Consulting, *Privacy Impact Assessment Report – Advanced Metering Infrastructure*, prepared for Victorian Department of Primary Industries, version 1.2, August 2011

Oakley Greenwood, *Review of AMI Benefits*, prepared for Victorian Department of Primary Industries, Final Report, July 2010

1. Australian Privacy Principles

The list below details the 13 APPs from [Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*](http://www.comlaw.gov.au/Details/C2012A00197/Html/Text#_Toc343175853), which amends the *Privacy Act 1988*.

## Part 1—Consideration of personal information privacy

### Australian Privacy Principle 1—open and transparent management of personal information

* 1. The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

*Compliance with the Australian Privacy Principles etc.*

* 1. An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity’s functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity’s compliance with the Australian Privacy Principles or such a code.

*APP Privacy policy*

* 1. An APP entity must have a clearly expressed and up to date policy (the ***APP privacy policy***) about the management of personal information by the entity.
  2. Without limiting sub clause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

*Availability of APP privacy policy etc.*

* 1. An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity’s website.

* 1. If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

### Australian Privacy Principle 2—anonymity and pseudonymity

* 1. Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.
  2. Sub clause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

## Part 2—Collection of personal information

### Australian Privacy Principle 3—collection of solicited personal information

*Personal information other than sensitive information*

* 1. If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.
  2. If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity’s functions or activities.

*Sensitive information*

* 1. An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity’s functions or activities; or

(b) sub clause 3.4 applies in relation to the information.

* 1. This sub clause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

*Means of collection*

* 1. An APP entity must collect personal information only by lawful and fair means.
  2. An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

*Solicited personal information*

* 1. This principle applies to the collection of personal information that is solicited by an APP entity.

### Australian Privacy Principle 4—dealing with unsolicited personal information

* 1. If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

* 1. The APP entity may use or disclose the personal information for the purposes of making the determination under sub clause 4.1.
  2. If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

* 1. If sub clause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

### Australian Privacy Principle 5—notification of the collection of personal information

* 1. At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in sub clause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

* 1. The matters for the purposes of sub clause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

## Part 3—Dealing with personal information

### Australian Privacy Principle 6—use or disclosure of personal information

*Use or disclosure*

* 1. If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

* 1. This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

* 1. This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

* 1. If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

*Written note of use or disclosure*

* 1. If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

*Related bodies corporate*

* 1. If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity’s primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

*Exceptions*

* 1. This principle does not apply to the use or disclosure by an organisation of:

(a) personal information for the purpose of direct marketing; or

(b) government related identifiers.

### Australian Privacy Principle 7—direct marketing

*Direct marketing*

* 1. If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

*Exceptions—personal information other than sensitive information*

* 1. Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

* 1. Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual’s attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

*Exception—sensitive information*

* 1. Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

*Exception—contracted service providers*

* 1. Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

*Individual may request not to receive direct marketing communications etc.*

* 1. If an organisation (the first organisation) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation;

or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

* 1. If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

*Interaction with other legislation*

* 1. This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

### Australian Privacy Principle 8—cross-border disclosure of personal information

* 1. Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

* 1. Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

### Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

*Adoption of government related identifiers*

* 1. An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

*Use or disclosure of government related identifiers*

* 1. An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation’s activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

*Regulations about adoption, use or disclosure*

* 1. This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

## Part 4—Integrity of personal information

### Australian Privacy Principle 10—quality of personal information

* 1. An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.
  2. An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

### Australian Privacy Principle 11—security of personal information

* 1. If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

* 1. If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

## Part 5—Access to, and correction of, personal information

### Australian Privacy Principle 12—access to personal information

*Access*

* 1. If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

* 1. If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

* 1. If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

* 1. The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

* 1. If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual; the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

* 1. Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

* 1. If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.
  2. If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

* 1. If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

* 1. If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

### Australian Privacy Principle 13—correction of personal information

Correction

* 1. If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

*Notification of correction to third parties*

* 1. If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

*Refusal to correct information*

* 1. If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

*Request to associate a statement*

* 1. If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

*Dealing with requests*

* 1. If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

1. Comparison of APPs to NPPs

The tables on the following pages compare the existing NPPs in column 1 with the new APPs in column 2. The third column contains relevant definitions in the Amending Act or in the APPs themselves.

Whenever possible, we have matched the new principles with the existing ones in a row. Where necessary, we have split sub-principles or exceptions and inserted them into new rows for ease of reference. Where this occurs, there is a bold and italicised reference to the sub-principle or exception in brackets, and the full text is cited later in the table. A blank in either the NPPs or the APPs column indicate that there is no equivalent provision in the relevant principles.

In completing this project we reviewed the recommendations in the Lockstep Report, based on the NPPs in the first column, against the APPs in the second column to identify any change in the principles that would impact on the recommendations. As the table is an overview of all principles, many of them were not relevant for the analysis of the recommendations in the Lockstep Report and the advice on whether the amended legislation would change the practical effect of those recommendations. The body of our report only considers the relevant amendments for our analysis and recommendations.

Table C.: High level comparison of APPs to NPPs

| **Current - *Privacy Act 1988* (Cth)**  **(Privacy Act)** | **Law reform - Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth) - (Amending Act)** | **Definitions under the Amending Act** |
| --- | --- | --- |
| **Information Privacy Principles (IPPs)**: Public sector; base line privacy standards that the Australian and ACT government agencies need to comply with in relation to *personal information* kept in their records.  **National Privacy Principles (NPPs)**: Private sector; base line privacy standards that some private sector organisations need to comply with in relation to personal information they hold. All health service providers in the private sector need to comply with these principles.  Small business operator exempted (see definition below), | Australian Privacy Principles (APPs): privacy principles applying to both Cth agencies and private sector organisations (*APP entities*).  The APPs do not apply to small business operators (see definition of *entity* and *APP entity* below) |  |
| Definition of Privacy Act s 6(1) ***agency*** means:  (a) a Minister; or  (b) a Department; or  (c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:  (i) an incorporated company, society or association; or  (ii) an organisation that is registered under the Fair Work (Registered Organisations) Act 2009 or a branch of such an organisation; or  (d) a body established or appointed by the Governor‑General, or by a Minister, otherwise than by or under a Commonwealth enactment; or  (e) a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department; or  (f) a person holding or performing the duties of an appointment, being an appointment made by the Governor‑General, or by a Minister, otherwise than under a Commonwealth enactment; or  (g) a federal court; or  (h) the Australian Federal Police; or  (ha) a Norfolk Island agency; or  (i) an eligible case manager; or  (j) the nominated AGHS company; or  (k) an eligible hearing service provider; or  (l) the service operator under the *Healthcare Identifiers Act 2010*.  Definition of ***organisations*** to which NPPs apply  Privacy Act s 6C(1) In this Act: *organisation* means:  (a) an individual; or  (b) a body corporate; or  (c) a partnership; or  (d) any other unincorporated association; or  (e) a trust;  that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.  S 6D *Small business* and *small business operator:* Annual turnover of $3 Million or under.  **Note**: Regulations may prescribe an instrumentality by reference to one or more classes of instrumentality. See subsection 13(3) of the *Legislative Instruments Act 2003*.  Example: Regulations may prescribe an instrumentality of a State or Territory that is an incorporated company, society or association and therefore not a State or Territory authority. | S 6 Privacy Act: definitions of *agency* and *organisation* unchanged | ***entity*** means:  a) an agency; or  (b) an organisation; or  (c) a small business operator  ***APP entity*** means an agency or organisation |
| Definition of *personal information*  S 6(1) *personal information* means 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 |  | S 36 Amending Act. New definition of ***personal information*:**  ***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:  (a) whether the information or opinion is true or not; and  (b) whether the information or opinion is recorded in a material form or not. |

Table C.: Detailed comparison of NPPs and APPs

| **Current – National Privacy Principles under the Privacy Act**  **(Numbers refer to NPPs)** | **Law reform – Australian Privacy Principles under the Amending Act**  **(Numbers refer to APPs)** | **Definitions under the Amending Act** |
| --- | --- | --- |
| **1. Collection** | **3 - collection of solicited personal information** |  |
|  | *Solicited personal information*  3.7 This principle [***APP 3***] applies to the collection of personal information that is solicited by an APP entity. |  |
| 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. | *Personal information other than sensitive information*  3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.  3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity’s functions or activities. | ***sensitive information*** means:  (a) information or an opinion about an individual’s:  (i) racial or ethnic origin; or  (ii) political opinions; or  (iii) membership of a political association; or  (iv) religious beliefs or affiliations; or  (v) philosophical beliefs; or  (vi) membership of a professional or trade association; or  (vii) membership of a trade union; or  (viii) sexual orientation or practices; or  (ix) criminal record;  that is also personal information; or  (b) health information about an individual; or  (c) genetic information about an individual that is not otherwise health information or;  (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or  (e) biometric templates. |
| 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way. | *Means of collection*  3.5 An APP entity must collect personal information only by lawful and fair means |  |
|  | **5 – notification of the collection of personal information** |  |
| 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. | 5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:  (a)  to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or  (b)  to otherwise ensure that the individual is aware of any such matters.  5.2 The matters for the purposes of subclause 5.1 are as follows:  (a)  the identity and contact details of the APP entity;  (b)  if:  (i) the APP entity collects the personal information from someone other than the individual; or  (ii) the individual may not be aware that the APP entity has collected the personal information;  the fact that the entity so collects, or has collected, the information and the circumstances of that collection;  (c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);  (d) the purposes for which the APP entity collects the personal information;  (e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;  (f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;  (g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;  (h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;  (i)  whether the APP entity is likely to disclose the personal information to overseas recipients;  (j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them. |  |
| 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual. | *Means of collection*  3.6 An APP entity must collect personal information about an individual only from the individual unless:  (a) if the entity is an agency:  (i) the individual consents to the collection of the information from someone other than the individual; or  (ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or  (b) it is unreasonable or impracticable to do so [***Applies to all APP entities***]. |  |
| 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. | See APP 3.6 and APP 5.2 above |  |
| **2 Use and disclosure** | **6 – use or disclosure of personal information** |  |
| 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 [***general prohibition on secondary disclosure***] 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) [***consent***]; or  (c) [***secondary purpose of direct marketing***] or  (d) [***health information***]  (e) [***threat to health or safety***] or  (ea) [***genetic information***]  (f) [***unlawful activity***]; or  (g) [**u*se or disclosure authorised or required by law***]; or  (h) [***enforcement related activity***] | *Use or disclosure*  6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the *primary purpose*), the entity must not use or disclose the information for another purpose (the *secondary purpose*) [***general prohibition on secondary disclosure***] unless:  (a) the individual has consented to the use or disclosure of the information; or  (b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.  6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:  (i) if the information is sensitive information—directly related to the primary purpose; or  (ii) if the information is not sensitive information—related to the primary purpose; or  (b) [***use or disclosure permitted by law***]; or  (c) [***permitted general situation***]; or  (d) [***permitted health situation***] or  (e) [***enforcement related activity***].  6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:  (a) the agency is not an enforcement body; and  (b) the information is biometric information or biometric templates; and  (c) the recipient of the information is an enforcement body; and  (d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph | ***permitted general situation***, see section Privacy Act s 16A.  ***permitted health situation***, see Privacy Act s 16B. |
| [***2.1.(b) Use and disclosure / Consent***]  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:  (b) the individual has consented to the use or disclosure; | 6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the *primary purpose*), the entity must not use or disclose the information for another purpose (the *secondary purpose*) unless:  (a) the individual has consented to the use or disclosure of the information;  See also APP 7.4 [***exception to general prohibition of direct marketing***]  *Exception –sensitive information*  Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose. |  |
|  | **7 – direct marketing** |  |
| [***2.1.(c) Use and disclosure/ Direct marketing***]  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:  (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 | *Prohibition on direct marketing*  7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.  **Note:** The prohibition against direct marketing will also apply to agencies engaging in commercial activities (see s 7A Privacy Act)  *Exceptions – personal information other than sensitive information*  APP 7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:  (a) the organisation collected the information from the individual; and  (b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and  (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and  (d) the individual has not made such a request to the organisation.  APP 7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:  (a) the organisation collected the information from:  (i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or  (ii) someone other than the individual; and  (b) either:  (i) the individual has consented to the use or disclosure of 1 the information for that purpose; or  (ii) it is impracticable to obtain that consent; and  (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and (d) in each direct marketing communication with the individual:  (i) the organisation includes a prominent statement that the individual may make such a request; or  (ii) the organisation otherwise draws the individual’s attention to the fact that the individual may make such a request; and  (e) the individual has not made such a request to the organisation. |  |
|  | *Exceptions – contracted service providers*  7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:  (a) the organisation is a contracted service provider for a Commonwealth contract; and  (b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and 27  (c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation. |  |
|  | *Individual may request not to receive direct marketing communications etc.*  7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:  (a) [***direct marketing by the first organisation***; ***see above***];  (b) for the purpose of facilitating direct marketing by other organisations;  the individual may:  (c) if paragraph (a) applies— [***see above***]; and  (d) if paragraph (b) applies— request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and  (e) request the first organisation to provide its source of the information.  7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:  (a)  if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and  (b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so. |  |
|  | *Interaction with other legislation*  7.8 This principle does not apply to the extent that any of the following apply:  (a) the *Do Not Call Register Act 2006*;  (b) the *Spam Act 2003*;  (c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations. |  |
|  | **6 – use or disclosure of personal information** |  |
| [***2.1(d) Use and disclosure/ Health information***]  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:  (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; | (*Use or disclosure*)  APP 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (d) the APP entity is an organisation and a *permitted health situation* exists in relation to the use or disclosure of the information by the entity; | ***permitted health situation*** has the meaning given by section 16B.  Privacy Act s 16B **Permitted health situations in relation to the collection, use or disclosure of health information**  *Collection—provision of a health service*  (1) A permitted health situation exists in relation to the collection by an organisation of health information about an individual if:  (a) the information is necessary to provide a health service to the individual; and  (b) either:  (i) the collection is required or authorised by or under an Australian law (other than this Act); or  (ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.  *Collection—research etc.*  (2) A permitted health situation exists in relation to the collection by an organisation of 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 about the individual that is de-identified information; and  (c) it is impracticable for the organisation to obtain the individual’s consent to the collection; and  (d) any of the following apply:  (i) the collection is required by or under an Australian law (other than this Act);  (ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;  (iii) the information is collected in accordance with guidelines approved under section 95A for the purposes of this subparagraph.  *Use or disclosure—research etc.*  (3) A permitted health situation exists in relation to the use or disclosure by an organisation of health information about an individual if:  (a) the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and  (b) it is impracticable for the organisation to obtain the individual’s consent to the use or disclosure; and  (c) the use or disclosure is conducted in accordance with guidelines approved under section 95A for the purposes of this paragraph; and  (d) in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.  *Disclosure—responsible person for an individual*  (5) A permitted health situation exists in relation to the disclosure by an organisation of health information about an individual if:  (a) the organisation provides a health service to the individual; and  (b) the recipient of the information is a responsible person for the individual; and  (c) the individual:  (i) is physically or legally incapable of giving consent to the disclosure; or  (ii) physically cannot communicate consent to the disclosure; and  (d) another individual (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  (e) 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  (f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d). |
| [***2.1(e) Use and disclosure / Threat to health or safety***]  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:  (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; | 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (c) a *permitted general situation* exists in relation to the use or disclosure of the information by the APP entity.  See Conditions re **Item 1** Table:  (a) it is unreasonable or impracticable to obtain the individual’s consent to the collection, use or disclosure; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety. | ***permitted general situation*** has the meaning given by section 16A.  16A **Permitted general situations in relation to the collection, use or disclosure of personal information**  (1) A permitted general situation exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:  (a) the entity is an entity of a kind specified in an item in column 1 of the table; and  (b) the item in column 2 of the table applies to the information or identifier; and  (c) such conditions as are specified in the item in column 3 of the table are satisfied. |
|  |  | s 16A(1) Column 3 items:  **Item 1**:  (a) it is unreasonable or impracticable to obtain the individual’s consent to the collection, use or disclosure; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.  **Item 2**:  (a) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.  **Item 3**:  (a) the entity reasonably believes that the collection, use or disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing; and  (b) the collection, use or disclosure complies with the rules made under subsection (2).  **Item 4**  The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.  **Item 5**  The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process.  **Item 6** (agency only):  The entity reasonably believes that the collection, use or disclosure is necessary for the entity’s diplomatic or consular functions or activities.  **Item 7** (defence force):  The entity reasonably believes that the collection, use or disclosure is necessary for any of the following occurring outside Australia and the external Territories:  (a) war or warlike operations;  (b) peacekeeping or peace enforcement;  (c) civil aid, humanitarian assistance, medical or civil emergency or disaster relief. |
| [***2.1 (ea) Use and disclosure of genetic information***]  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:  (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; | 6.2(d) APP 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (d) the APP entity is an organisation and a *permitted health situation* exists in relation to the use or disclosure of the information by the entity; | ***permitted health situation*** has the meaning given by section 16B.  Privacy Act s 16B **Permitted health situations in relation to the collection, use or disclosure of health information**  *Use or disclosure—genetic information*  (4) A permitted health situation exists in relation to the use or disclosure by an organisation of genetic information about an individual (the first individual) if:  (a) the organisation has obtained the information in the course of providing a health service to the first individual; and  (b) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual; and  (c) the use or disclosure is conducted in accordance with guidelines approved under section 95AA; and  (d) in the case of disclosure—the recipient of the information is a genetic relative of the first individual. |
| [***2.1(f) Use and disclosure / Unlawful activity***]  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:  (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; | 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (c) a *permitted general situation* exists in relation to the use or disclosure of the information by the APP entity.  See Conditions re **Item 2** Table:  (a) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter. | ***permitted general situation*** has the meaning given by section 16A.  16A **Permitted general situations in relation to the collection, use or disclosure of personal information**  (1) A permitted general situation exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:  (a) the entity is an entity of a kind specified in an item in column 1 of the table; and  (b) the item in column 2 of the table applies to the information or identifier; and  (c) such conditions as are specified in the item in column 3 of the table are satisfied. |
| [***2.1(g) Use and disclosure / Use or disclosure authorised or required by law***]  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:  (g) the use or disclosure is required or authorised by or under law | [**6.2(b)** ***Use or disclosure permitted by law***]  6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; |  |
| [***2.1(h) Use and disclosure / Enforcement related activity***]  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:  (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. | [***6.2(e) enforcement related activity***]  6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.  See APP6.2.(c) and Privacy Act s 16A,Item 4:  The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim. |  |
| 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h) [***Enforcement related activity***], it must make a written note of the use or disclosure. | *Written note of use or disclosure*  6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity 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. | *Related bodies corporate*  6.6 If:  (a) an APP entity is a body corporate; and  (b) the entity collects personal information from a related body corporate;  this principle [***APP* 6**] applies as if the entity’s primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information |  |
|  | *Exceptions*  6.7 This principle [***i.e. APP 6; see EM p. 81***]does not apply to the use or disclosure by an organisation of:  (a)  personal information for the purpose of direct marketing [***see APP 7***]; or  (b)  government related identifiers. [***see APP 9***] |  |
| 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). | 6.2(d) APP 6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:  (d) the APP entity is an organisation and a *permitted health situation* exists in relation to the use or disclosure of the information by the entity; | ***permitted health situation*** has the meaning given by section 16B.  Privacy Act s 16B **Permitted health situations in relation to the collection, use or disclosure of health information**  *Disclosure—responsible person for an individual*  (5) A permitted health situation exists in relation to the disclosure by an organisation of health information about an individual if:  (a) the organisation provides a health service to the individual; and  (b) the recipient of the information is a responsible person for the individual; and  (c) the individual:  (i) is physically or legally incapable of giving consent to the disclosure; or  (ii) physically cannot communicate consent to the disclosure; and  (d) another individual (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  (e) 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  (f) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (d). |
| 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. |  | Sch 1 Item 40 (s 6(1)) ***responsible person*** has the meaning given by section 6AA.  s **6AA Meaning of responsible person**  (1) A responsible person for an individual is:  (a) a parent of the individual; or  (b) a child or sibling of the individual if the child or sibling is at least 18 years old; or  (c) a spouse or de facto partner of the individual; or  (d) a relative of the individual if the relative is:  (i) at least 18 years old; and  (ii) a member of the individual’s household; or  (e) a guardian of the individual; or  (f) a person 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. |  | s **6AA Meaning of responsible person**  (2) In this section:  ***child***: without limiting who is a child of an individual for the purposes of subsection (1), each of the following is a child of an individual:  (a) an adopted child, stepchild, ex nuptial child or foster child of the individual;  (b) someone who is a child of the individual within the meaning of the Family Law Act 1975.  ***parent***: without limiting who is a parent of an individual for the purposes of subsection (1), someone is a parent of an individual if the individual is his or her child because of the definition of child in this subsection.  ***relative*** of an individual (the first individual) means a grandparent, grandchild, uncle, aunt, nephew or niece of the first individual and for this purpose, relationships to the first individual may also be traced to or through another individual who is:  (a) a de facto partner of the first individual; or  (b) the child of the first individual because of the definition of child in this subsection.  ***sibling*** of an individual includes:  (a) a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister of the individual; and  (b) another individual if a relationship referred to in paragraph (a) can be traced through a parent of either or both of the individuals.  ***stepchild***: without limiting who is a stepchild of an individual, someone is a stepchild of an individual if he or she would be the individual’s stepchild except that the individual is not legally married to the individual’s de facto partner. |
| **3. Data quality** | **10 – Quality of personal information** |  |
| 3. 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. | 10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up‑to‑date and complete.  10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up‑to‑date, complete and relevant. |  |
| **4 Data security** | **11 Security of personal information** |  |
| 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. | 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:  (a)  from misuse, **interference** and loss; and  (b)  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. | 11.2 If:  (a) an APP entity holds personal information about an individual; and  (b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and  (c) the information is not contained in a Commonwealth record; and  (d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;  the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de‑identified. |  |
| **5. Openness** | **1. Open and transparent management of personal information** |  |
|  | 1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way. |  |
|  | *Compliance with the Australian Privacy Principles etc.*  1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity’s functions or activities that:  (a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and  (b) will enable the entity to deal with inquiries or complaints from individuals about the entity’s compliance with the Australian Privacy Principles or such a code. |  |
| 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. | 1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity. |  |
| 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. | 1.4 Without limiting sub clause 1.3, the APP privacy policy of the APP entity must contain the following information:  (a) the kinds of personal information that the entity collects and holds;  (b) how the entity collects and holds personal information;  (c) the purposes for which the entity collects, holds, uses and discloses personal information;  (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;  (e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;  (f) whether the entity is likely to disclose personal information to overseas recipients;  (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy. |  |
|  | *Availability of APP privacy policy etc.*  1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:  (a) free of charge; and  (b) in such form as is appropriate.  Note: An APP entity will usually make its APP privacy policy available on the entity’s website.  1.6 If a person or body requests a copy of the APP privacy policy of an  APP entity in a particular form, the entity must take such steps as  are reasonable in the circumstances to give the person or body a copy in that form. |  |
| **6. Access and correction** | **12. Access to personal information** |  |
| 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 [***see exceptions below***]:  (a) [***serious and imminent threat to health or health***; or  (b) [***health information - serious threat to the life or health***]; or  (c) [ ***unreasonable impact upon the privacy of others***]; or  (d) [***frivolous or vexatious request***]; or  (e) [***legal proceedings between the organisation and the individual***]; or  (f) [***negotiations with the individual***]; or  (g) [***unlawfulness***]; or  (h) [***denying access is required or authorised by or under law***]; or  (i) [***prejudice to investigation of possible unlawful activity***]; or  (j) [***prejudice to law enforcement activities***]: or  (k) [***security of Australia***]. | *Access*  12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.  *Exception to access—agency*  12.2  If:  (a)  the APP entity is an agency; and  (b)  the entity is required or authorised to refuse to give the individual access to the personal information by or under:  (i)  the Freedom of Information Act; or  (ii)  any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;  then, despite sub clause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access. |  |
| [***Exception to obligation to provide access / Serious and imminent threat to health or health***]  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; | *Exceptions to access – organisation*  12.3  If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (a)  the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; |  |
| [***Exception to obligation to provide access / Health information -Serious and threat to health or health***]  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:  (b) in the case of health information' -providing access would pose a serious threat to the life or health of any individual; |  |
| ***Exception to obligation to provide access / Unreasonable impact upon the privacy of others***  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:  (c) providing access would have an unreasonable impact upon the privacy of other individuals; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (b) giving access would have an unreasonable impact on the privacy of other individuals; |  |
| [***Exception to obligation to provide access / Frivolous or vexatious request***]  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:  (d) the request for access is frivolous or vexatious; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (c)  the request for access is frivolous or vexatious; |  |
| [***Exception to obligation to provide access / legal proceedings between the organisation and the individual***]  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:  (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; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; |  |
| [***Exception to obligation to provide access / Negotiations with the individual***]  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:  (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; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; |  |
| [***Exception to obligation to provide access / Unlawfulness***]  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:  (g) providing access would be unlawful; or | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (f) giving access would be unlawful; |  |
| [***Exception to obligation to provide access /***  ***Denying access is required or authorised by or under law***]  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:  (h) denying access is required or authorised by or under law; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (g) denying access is required or authorised by or under an Australian law or a court/tribunal order |  |
| [***Exception to obligation to provide access /***  ***Prejudice to investigation of possible unlawful activity***]  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:  (i) providing access would be likely to prejudice an investigation of possible unlawful activity; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (h) both of the following apply:  (i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity’s functions or activities has been, is being or may be engaged in;  (ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; |  |
| [***Exception to obligation to provide access /*** ***Prejudice to law enforcement activities***]  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:  (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; | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; |  |
| [***Exception to obligation to provide access / Security of Australia***]  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:  (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.* | *Exceptions to access – organisation*  12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:  (j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision making process |  |
|  | *Dealing with requests for access*  12.4 The APP entity must:  (a) respond to the request for access to the personal information:  (i) if the entity is an agency—within 30 days after the request is made; or  (ii) if the entity is an organisation—within a reasonable period after the request is made; and  (b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so. |  |
| 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. | *Other means of access*  12.5 If the APP entity refuses:  (a) to give access to the personal information because of subclause 12.2 or 12.3; or  (b) to give access in the manner requested by the individual;  the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.  12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary. |  |
| 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. | *Access charges*  12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.  12.8 If:  (a)  the APP entity is an organisation; and  (b)  the entity charges the individual for giving access to the personal information; the charge must not be excessive and must not apply to the making of the request. |  |
|  | **13 – correction of personal information** |  |
| 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. | *Correction*  13.1  If:  (a) an APP entity holds personal information about an individual; and  (b) either:  (i) the entity is satisfiedthat, having regard to a purpose for which the information is held, the information is inaccurate, out‑of‑date, incomplete, irrelevant or misleading; or  (ii) the individual requests the entity to correct the information;  the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up‑to‑date, complete, relevant and not misleading. |  |
|  | *Notification of correction to third parties*  13.2 If:  (a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and  (b) the individual requests the entity to notify the other APP entityof the correction;  the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so. |  |
| 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. | *Request to associate a statement*  13.4 If:  (a) the APP entity refuses to correct the personal information as requested by the individual; and  (b)  the individual requests the entity to associate with the information a statement that the information is inaccurate, out‑of‑date, incomplete, irrelevant or misleading;  the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information. |  |
|  | **12 – access to personal information** |  |
| 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.  See also 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. | *Refusal to give access*  12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:  (a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and  (b) the mechanisms available to complain about the refusal; and  (c) any other matter prescribed by the regulations.  12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.  *Refusal to correct information*  13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:  (a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and  (b) the mechanisms available to complain about the refusal; and  (c) any other matter prescribed by the regulations. |  |
|  | *Dealing with requests*  13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:  (a) must respond to the request:  (i) if the entity is an agency—within 30 days after the request is made; or  (ii) if the entity is an organisation—within a reasonable period after the request is made; and  (b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be). |  |
| **7. Identifiers** | **9 – adoption, use or disclosure of government related 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. | *Adoption of government related identifiers*  9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:  (a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or  (b) subclause 9.3 applies in relation to the adoption.  **Note**: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A. |  |
| 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). | *Regulations about adoption, use or disclosure*  9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:  (a) the identifier is prescribed by the regulations; and  (b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and  (c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations. |  |
| 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) [***any of the exceptions in par 2.1(e) to 2.1(h) re secondary use apply***]; or  (c) [***prescribed organisation in prescribed circumstances***]  **Note**: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2) and (3). | *Use or disclosure of government related identifiers*  9.2 An organisation must not use or disclose a government related identifier of an individual unless:  (a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation’s activities or functions; or  (b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority;  (c) [***permitted by law or order***]; or  (d) [***general permitted situation***];  (e) [***enforcement related activities***]  (f) [***9.3 Regulations***] |  |
| [***Any of the exceptions in par 2.1(e) to 2.1(h) re secondary use apply***]  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:  (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or  2.1(e) [***2.1(e) Use and disclosure / Threat to health or safety***]  2.1.(ea) [***2.1 (ea) Use and disclosure of genetic information***]  2.1(f) [***2.1(f) Use and disclosure / Unlawful activity***]  2.1(g) [***2.1(g) Use and disclosure / Use or disclosure authorised or required by law***]  2.1(h) [***2.1(h) Use and disclosure / Enforcement related activity***] | *Use or disclosure of government related identifiers*  9.2 An organisation must not use or disclose a government related identifier of an individual unless:  (c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or  (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier;  (e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or | s 16A (1) Item 4  The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim.  s 16A(1) Item 5  The collection, use or disclosure is reasonably necessary for the purposes of a confidential alternative dispute resolution process. |
| [***prescribed organisation in prescribed circumstances***]  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:  (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances. | *Use or disclosure of government related identifiers*  9.2 An organisation must not use or disclose a government related identifier of an individual unless:  (f) sub clause 9.3 applies in relation to the use or disclosure |  |
| 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. |  | Sch 1 Item 23 (s 6(1))  ***government related identifier*** of an individual means an identifier of the individual that has been assigned by  (a) an agency; or  (b) a State or Territory authority; or  (c) an agent of an agency, or a State or Territory authority, acting in its capacity as agent; or  (d) a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract. |
| **8. Anonymity** | **2 – Anonymity and pseudonymity** |  |
| 8. Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation. | 2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.  2.2 Subclause 2.1 does not apply if, in relation to that matter:  (a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or  (b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym. |  |
| **9. Transborder data flows** | **8 - Cross‑border disclosure of personal information** |  |
| 9. 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) [c***onsent***]; 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. | 8.1 Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***):  (a) who is not in Australia or an external Territory; and  (b) who is not the entity or the individual;  the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.  **Note** In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.  8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:  (a) the entity reasonably believes that:  (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and  (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or  or  (b) [***consent***]; or  (c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or  (d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or  (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or  (f) the entity is an agency and both of the following apply:  (i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;  (ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body. | S 16C **Acts and practices of overseas recipients of personal information**  (1) This section applies if:  (a) an APP entity discloses personal information about an individual to an overseas recipient; and  (b) Australian Privacy Principle 8.1 applies to the disclosure of the information; and  (c) the Australian Privacy Principles do not apply, under this Act, to an act done, or a practice engaged in, by the overseas recipient in relation to the information; and  (d) the overseas recipient does an act, or engages in a practice, in relation to the information that would be a breach of the Australian Privacy Principles (other than Australian Privacy Principle 1) if those Australian Privacy Principles so applied to that act or practice.  (2) The act done, or the practice engaged in, by the overseas recipient is taken, for the purposes of this Act:  (a) to have been done, or engaged in, by the APP entity; and  (b) to be a breach of those Australian Privacy Principles by the APP entity. |
| [***transborder data flow – consent***]  9. 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:  (b) the individual consents to the transfer | 8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:  (b) both of the following apply:  (i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;  (ii) after being so informed, the individual consents to the disclosure; |  |
| **10 Sensitive information** | **3 – Collection of solicited personal information** |  |
| 10.1 An organisation must not collect sensitive information about an individual unless:  (a) the individual has consented; or  (b) [***required by law***]; or  (c) [***serious threat to life or health***]  (d) [***activities of a non-profit organisation***]; or  (e) [***claim***] | *Sensitive information*  3.3 An APP entity must not collect sensitive information about an individual unless:  (a) the individual consents to the collection of the information and:  (i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or  (ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity’s functions or activities; or  (b) subclause 3.4 applies in relation to the information.  3.4 This subclause applies in relation to sensitive information about an individual if:  (a) [***law or court order***];  (b) [***permitted general situation; Privacy Act s 16A***];  (c)  the APP entity is an organisation and a permitted health situation [***Privacy Act s 16B***] exists in relation to the collection of the information by the entity; or  (d) the APP entity is an enforcement body and the entity reasonably believes that:  (i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or  (ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities; or  (e) [***activities of non-profit organisations***] |  |
| [***Exception to prohibition to collect sensitive information / Required by law***]  10.1 An organisation must not collect sensitive information about an individual unless:  (b) the collection is required by law; | 3.4 This subclause applies in relation to sensitive information about an individual if:  (a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; |  |
| [***Exception to prohibition to collect sensitive information / Serious threat to life or health***]  10.1 An organisation must not collect sensitive information about an individual unless:  (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; | 3.4 This subclause applies in relation to sensitive information about an individual if:  (b) a permitted general situation exists in relation to the collection of the information by the APP entity.  See Conditions re **Item 1** Table:  (a) it is unreasonable or impracticable to obtain the individual’s consent to the collection, use or disclosure; and  (b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety. | ***permitted general situation*** has the meaning given by section 16A.  16A **Permitted general situations in relation to the collection, use or disclosure of personal information**  (1) A permitted general situation exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:  (a) the entity is an entity of a kind specified in an item in column 1 of the table; and  (b) the item in column 2 of the table applies to the information or identifier; and  (c) such conditions as are specified in the item in column 3 of the table are satisfied. |
| [***Exception to prohibition to collect sensitive information / Activities of non-profit organisation***]  10.1 An organisation must not collect sensitive information about an individual unless:  (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 | 3.4 This subclause applies in relation to sensitive information about an individual if:  (e) the APP entity is a non‑profit organisation and both of the following apply:  (i) the information relates to the activities of the organisation;  (ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities. |  |
| [***Exception to prohibition to collect sensitive information / Claim***]  10.1 An organisation must not collect sensitive information about an individual unless:  (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim. | 3.4 This subclause applies in relation to sensitive information about an individual if:  (b) a permitted general situation exists in relation to the collection of the information by the APP entity.  See Conditions re **Item 4** Table:  The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim. | ***permitted general situation*** has the meaning given by section 16A.  16A **Permitted general situations in relation to the collection, use or disclosure of personal information**  (1) A permitted general situation exists in relation to the collection, use or disclosure by an APP entity of personal information about an individual, or of a government related identifier of an individual, if:  (a) the entity is an entity of a kind specified in an item in column 1 of the table; and  (b) the item in column 2 of the table applies to the information or identifier; and  (c) such conditions as are specified in the item in column 3 of the table are satisfied. |
| 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. | 3.4 This subclause applies in relation to sensitive information about an individual if:  (c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; | ***permitted health situation*** has the meaning given by section 16B.  Privacy Act s 16B **Permitted health situations in relation to the collection, use or disclosure of health information**  *Collection—provision of a health service*  (1) A permitted health situation exists in relation to the collection by an organisation of health information about an individual if:  (a) the information is necessary to provide a health service to the individual; and  (b) either:  (i) the collection is required or authorised by or under an Australian law (other than this Act); or  (ii) the information is collected 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. | 3.4 This subclause applies in relation to sensitive information about an individual if:  (c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; | ***permitted health situation*** has the meaning given by section 16B.  Privacy Act s 16B **Permitted health situations in relation to the collection, use or disclosure of health information**  *Collection—research etc.*  16B(2) A permitted health situation exists in relation to the collection by 20 an organisation of 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 about the individual that is de-identified information; and  (c) it is impracticable for organisation to obtain the individual’s consent to the collection; and  (d) any of the following apply:  (i) the collection is required by or under an Australian law (other than this Act);  (ii) the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation;  (iii) the information is collected in accordance with guidelines approved 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. | 6.4 If:  (a) the APP entity is an organisation; and  (b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;  the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2. |  |
| 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. |  | Amending Act Sch 1 Item 31  ***non-profit organisation*** means an organisation:  (a) that is a non-profit organisation; and  (b) that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes. |
|  | 4. **Dealing with unsolicited information** |  |
|  | 4.1 If:  (a) an APP entity receives personal information; and  (b) the entity did not solicit the information;  the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under AustralianPrivacy Principle 3 if the entity had solicited the information.  4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.  4.3 If:  (a) the APP entity determines that the entity could not have collected the personal information; and  (b) the information is not contained in a Commonwealth record;  the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de‑identified.  4.4 If sub clause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under AustralianPrivacy Principle 3. |  |

1. Detailed analysis of energy market regulations

As outlined in Section 2.2 we identified those regulatory instruments of Queensland, New South Wales, the ACT, Tasmania, South Australia and Western Australia (as identified by the Commonwealth) and the national electricity instruments which relate to electricity metering datato assess whether any of the obligations under, or rights granted by, those regulatory instruments were inconsistent with the Lockstep recommendations.

The table on the following pages outline the detailed findings by jurisdiction and national (NEM) regulatory instruments. The table is further divided into four columns – ‘collection of data’, ‘use and disclosure of data’, ‘data security’ and ‘access to data’ – to reflect the different NPPs considered by the Lockstep report.

Table D.1: Analysis of energy market regulatory instruments - National

## NATIONAL (NEM JURISDICTIONS ONLY)

| **Instrument** | **Collection of data** | **Use and disclosure of data** | **Data security (storage and protection)** | **Access to data** |
| --- | --- | --- | --- | --- |
| ***National Electricity Law*** | The NEL contains provisions for information to be gathered by, or provided to authorities (AEMO, AER, AEMC). This information may include metering data. | Generally these authorities are authorised to use information for statutory purposes and to disclose it, including confidential information, in certain circumstances as set out.  These circumstances include with consent, if there is no person identified, where the public benefit outweighs the private detriment, if required by law or, in AEMO’s case, for the safety, reliability and security of the system. | Generally these authorities take all reasonable measures to protect information from unauthorised use or unauthorised disclosure of information. | \* Nothing relevant |
| ***National Electricity Rules***  The principal provisions are extracted here. Other provisions cross refer to these.  For example, the responsibilities of the Responsible Person include compliance with clauses 7.8.2 and 7.7(a). | \* Nothing relevant | **8.6.1 Confidentiality**  (a) Each *Registered Participant* must use all reasonable endeavours to keep confidential any *confidential information* that comes into the possession or control of the *Registered Participant* or of which the *Registered Participant* becomes aware.  (b) A *Registered Participant*:  (1) must not disclose *confidential information* to any person except as permitted by the *Rules*;  (2) must only use or reproduce *confidential information* for the purpose for which it was disclosed or another purpose contemplated by the *Rules*; and  (c) Each *Registered Participant* must use all reasonable endeavours:  (1) to prevent unauthorised access to *confidential information* which is in the possession or control of that *Registered Participant*; and  (2) to ensure that any person to whom it discloses *confidential information* observes the provisions of this rule 8.6 in relation to that information.  **8.6.2 Exceptions**  This rule 8.6 does not prevent:  (a) (public domain): the disclosure, use or reproduction of information if the relevant information is at the time generally and publicly available other than as a result of breach of confidence by the *Registered Participant* who wishes to disclose, use or reproduce the information or any person to whom the *Registered Participant* has disclosed the information;  (b) (employees and advisers): the disclosure of information by a *Registered Participant* or the *Registered Participant's Disclosees* to:  (1) an employee or officer of the *Registered Participant* or a *related body corporate* of the *Registered Participant*; or  (2) a legal or other professional adviser, auditor or other consultant (in this clause 8.6.2(b) called Consultants) of the *Registered Participant*, which require the information for the purposes of the *Rules*, or for the purpose of advising the *Registered Participant* or the *Registered Participant's Disclosee* in relation thereto;  (c) (consent): the disclosure, use or reproduction of information with the consent of the person or persons who provided the relevant information under the *Rules*;  (d) (law): the disclosure, use or reproduction of information to the extent required by law or by a lawful requirement of:  (1) any government or governmental body, authority or agency having jurisdiction over a *Registered Participant* or its *related bodies corporate*; or  (2) any stock exchange having jurisdiction over a *Registered Participant* or its *related bodies corporate*;  (e) (disputes): the disclosure, use or reproduction of information if required in connection with legal proceedings, arbitration, expert determination or other dispute resolution mechanism relating to the *Rules*, or for the purpose of advising a person in relation thereto;  (f) (trivial): the disclosure, use or reproduction of information which is trivial in nature;  (g) (safety): the disclosure of information if required to protect the safety of personnel or equipment;  (h) (potential investment): the disclosure, use or reproduction of information by or on behalf of a *Registered Participant* to the extent reasonably required in connection with the *Registered Participant's* financing arrangements, investment in that *Registered Participant* or a disposal of that *Registered Participant's* assets;  (i) (regulator): the disclosure of information to the *AER*, the *AEMC* or the *ACCC* or any other regulatory authority having jurisdiction over a *Registered Participant*, pursuant to the *Rules* or otherwise;  (j) (reports): the disclosure, use or reproduction of information of an historical nature in connection with the preparation and giving of reports under the *Rules*;  (k) (aggregate sum): the disclosure, use or reproduction of information as an unidentifiable component of an aggregate sum;  (l) (profile): the publication of a *profile*.  **8.6.3 Conditions**  In the case of a disclosure under clauses 8.6.2(b), or 8.6.2(h), prior to making the disclosure the *Registered Participant* that wishes to make the disclosure must inform the proposed recipient of the confidentiality of the information and must take appropriate precautions to ensure that the proposed recipient keeps the information confidential in accordance with the provisions of this rule 8.6 and does not use the information for any purpose other than that permitted under clause 8.6.1. | **7.8 Security of Metering Installations and Data**  **7.8.2 Security controls**  (a) The *responsible person* must ensure that *energy data* held in the *metering installation* is protected from direct local or remote electronic access by suitable password and security controls in accordance with paragraph (c).  (b) The *Metering Provider* must keep records of electronic access passwords secure.  (c) The *Metering Provider* must allocate 'read-only' passwords to *Market Participants*, *Local Network Service Providers* and *AEMO*, except where separate 'read-only' and 'write' passwords are not available, in which case the *Metering Provider* must allocate a password to *AEMO* only. For the avoidance of doubt, a *financially responsible Market Participant* may allocate that 'read-only' password to a customer who has sought access to its *energy data* or *metering data* in accordance with rule 7.7(a)(7).  (d) The *Metering Provider* must hold 'read-only' and 'write' passwords.  (e) The *Metering Provider* must forward a copy of the passwords held under paragraph (d) to *AEMO* on request by *AEMO* for *metering installations* types 1, 2,3 and 4.  (f) *AEMO* must hold a copy of the passwords referred to in paragraph (e) for the sole purpose of revealing them to a *Metering Provider* in the event that the passwords cannot be obtained by the *Metering Provider* by any other means.  (g) Subject to the authorisation of the *responsible person* which is for the purpose of managing congestion in accordance with rule 7.7(c1), if a *retail customer* of a *financially responsible Market Participant* requests a ‘read-only’ password, the *financially responsible Market Participant* must:  (1) obtain a ‘read-only’ password from the *Metering Provider* in accordance with paragraph (c); and  (2) provide a ‘read-only’ password to the customer within 10 *business days*.  (h) The *responsible person* referred to in paragraph (g) must not unreasonably withhold the authorisation required by the *financially responsible Market Participant*.  (i) The *Metering Provider* must allocate suitable passwords to the *Metering Data Provider* that enables the *Metering Data Provider* to collect the *metering data* and to maintain the clock of the *metering installation* in accordance with rule 7.12.  (j) The *Metering Data Provider* must keep all *metering installation* passwords secure and not make the passwords available to any other person.  **7.10 Confidentiality**  *Energy data*, *metering data*, *NMI Standing Data*, information in the *metering register* and passwords are confidential and are to be treated as *confidential information* in accordance with the *Rules*.  **7.11.3 Data management and storage**  (a) *Metering Data Providers* must:  (1) retain *metering data* for all relevant *metering installations* in the *metering data services database*:  (i) online in an accessible format for at least 13 months;  (ii) following the retention under subparagraph (1)(i), in an accessible format for an overall period of not less than 7 years; and  (2) archive in an accessible format for a period of 7 years:  (i) *metering data* in its original form collected from the *metering installation*;  (ii) records of each substitution to *metering data* in respect of a *metering installation*.  **8.6.6 AEMO information**  *AEMO* must develop and, to the extent practicable, implement a policy:  (a) to protect information which it acquires pursuant to its various functions from use or access which is contrary to the provisions of the *Rules*;  (b) to disseminate such information in accordance with its rights, powers and obligations in a manner which promotes the orderly operation of any *market*; and  (c) to ensure that *AEMO*, in undertaking any trading activity except the procurement of *ancillary services*, does not make use of such information unless the information is also available to other *Registered Participants*. | **7.7 Entitlement to metering data and access to metering installation**  (a) The only persons entitled to access *energy data* or to receive *metering data*, *NMI Standing Data*, *settlements ready data* or data from the *metering register* for a *metering installation* are:  (1) *Registered Participants* with a financial interest in the *metering installation* or the *energy* measured by that *metering installation*;  (2) *Metering Providers* who have an agreement to service the *metering installation*, in which case the entitlement to access is restricted to allow authorised work only;  (3) *financially responsible Market Participants* in accordance with the meter churn procedures developed under clause 7.3.4(j);  (4) the *Network Service Provider* or providers associated with the *connection point*;  (5) *AEMO* and its authorised agents;  (6) an Ombudsman in accordance with paragraphs (d), (e) and (f);  (7) a *financially responsible Market Participant’s* customer upon request by that customer to the *financially responsible Market Participant* for information relating to that customer’s *metering installation*;  (8) the *AER* or *Jurisdictional Regulators* upon request to *AEMO*; and  (9) *Metering Data Providers* who have been engaged to provide *metering data services* for that *metering installation* or in accordance with clause 7.14.1A(c)(6).  **7.9 Processing of Metering Data for Settlements Purposes**  **7.9.1 Metering databases**  (a) *AEMO* must create, maintain and administer a *metering database* (either directly or under a contract for provision of the database) containing information for each *metering installation* registered with *AEMO*.  (c) The *metering database* must have the capacity for electronic access by relevant *Market Participants* and *Network Service Providers*.  (d) The *metering database* must include *metering data*, *settlements ready data*, and information for each *metering installation* registered with *AEMO* in accordance with rule 7.5.  (e) Rights of access to data held within the *metering database* are set out in rule 7.7. |
| ***National Energy Retail Law*** | The NERL contains provisions for information to be collected by or given to the AER. This information may include metering data. | The AER is authorised to disclose information, including confidential information, in certain circumstances as set out including with consent or where the public benefit outweighs the private detriment.  **174—Authorised disclosure of information**  To the extent that the information is personal information within the meaning of the Privacy Act 1988 of the Commonwealth or of any Act of a participating jurisdiction relating to privacy—  (a) disclosure of that information to the AER, AEMO, a distributor or a designated RoLR for or in connection with the RoLR scheme is authorised by this Law; and  (b) use of that information for or in connection with the RoLR scheme is authorised by this Law. | \* Nothing relevant | \* Nothing relevant |
| ***National Energy Retail Rules* 2012** | \* Nothing relevant | **102 Enquiries or complaints relating to the distributor** (1) If a person makes an enquiry or complaint to a retailer about an issue relating to a distribution system or customer connection services (other than a fault, an emergency, a planned interruption or an unplanned interruption), the retailer must—  (a) if the enquiry or complaint is made by telephone—refer the person to the relevant distributor’s enquiry or complaints telephone number where practicable; or  (b) otherwise, as soon as practicable, but no later than the next business day after receiving the enquiry or complaint, provide the relevant distributor with the details of the enquiry or the complaint, including contact details of both the person making the enquiry or complaint and the person who received the enquiry or complaint.  (2) If a retailer requests a distributor to provide information about a shared customer’s energy consumption, the distributor must use its best endeavours to provide the information to the retailer at no cost and in a timely manner to allow the retailer to carry out its obligations to provide information to its customer.  **171 Distributor obligations—electricity consumption information** Distributors must, for the purpose of the electricity consumption benchmarks [for residential customers under a customer retail contract provided by the AER to retailers and published on its website], provide information to the AER in such manner and form as may be requested by the AER.  **Schedule 1 – Model Terms and Conditions for Standard Retail Contracts**  **Clause 18 Privacy Notice**  We will comply with all relevant privacy legislation in relation to your personal information. You can find a summary of our privacy policy on our website. If you have any questions, you can contact out privacy officer.  **Clause 22 Retailer of Last Resort Event**  If we are no longer entitled by law to sell energy to you due to a Retailer of Last Resort (RoLR) event occurring in relation to us, we are required under the National Energy Retail Law and the Rules to provide relevant information (including your name, billing address and metering identifier) to the entity appointed as the relevant designated retailer for the RoLR event and this contract will come to an end. | \* Nothing relevant | **28 Historical billing information (SRC and MRC)** (1) A retailer must promptly provide a small customer with historical billing data for that customer for the previous 2 years on request.  **86 Provision of information** A distributor must, on request by a customer or a customer’s retailer, provide information about the customer’s energy consumption or the distributor’s charges...  **132 Consumption information to be provided** (1) On request, a retailer must promptly provide a small customer with the following information relating to the customer’s premises— (a) total energy consumption;  (b) average daily consumption;  **129 System requirements** (2) System display The prepayment meter system must display— (a) the financial balance of the prepayment meter system, accurate to within $1.00 of the actual balance; and (b) whether the prepayment meter system is operating in normal credit or emergency credit mode; and (c) current consumption information (in both KWh or MJ and $AUD).  **Schedule 1 – Model Terms and Conditions for Standard Retail Contracts**  **Clause 9.4 Your historical billing information**  Upon request, we must give you information about your billing history for the previous 2 years free of charge. However, we may charge you if we have already given you this information in the previous 12 months, or if you require information going back more than 2 years. |

## SOUTH AUSTRALIA

Table D.2: Analysis of energy market regulatory instruments – South Australia

| **Instrument** | **Collection of data** | **Use and disclosure of data** | **Data security (storage and protection)** | **Access to data** |
| --- | --- | --- | --- | --- |
| **Essential Services Commission Act 2002 (SA)** | **29—Commission's power to require information**  (1) The Commission may, by written notice, require a person to give the Commission, within a time and in a manner stated in the notice (which must be reasonable), information in the person's possession that the Commission reasonably requires for the performance of the Commission's functions.  (1a) The power of the Commission to require information includes (without limitation) power to require a NERL retailer required to comply with Part 6A of the *Electricity* *Act 1996* or Part 5A of the *Gas Act 1997*—  (a) to conduct an audit, in a manner approved by the Commission, of the NERL retailer's compliance with the relevant Part; and  (b) to report the results of the audit to the Commission.  (2) A person must comply with a requirement under this section.  (3) A person cannot be compelled to give information under this section if the information might tend to incriminate the person of an offence.  (4) In this section—  ***NERL retailer*** has the same meaning as in the *Electricity Act 1996* or the *Gas Act 1997* (as the context requires). | **30—Obligation to preserve confidentiality**  (1) Information gained under this Part that—  (a) could affect the competitive position of a regulated entity or other person; or  (b) is commercially sensitive for some other reason, is, for the purposes of this Act, confidential information and a person performing a function under this Act or a relevant industry regulation Act is guilty of an offence if the person discloses such information otherwise than as authorised under this section.  (2) Confidential information may be disclosed if—  (a) the disclosure is made to another who is also performing a function under this Act or a relevant industry regulation Act; or  (b) the disclosure is made with the consent of the person who gave the information or to whom the information relates; or  (c) the disclosure is authorised or required under any other Act or law; or  (d) the disclosure is authorised or required by a court or tribunal constituted by law; or  (e) the disclosure is authorised by regulation.  (3) The Commission may disclose confidential information if the Commission is of the opinion that the public benefit in making the disclosure outweighs any detriment that might be suffered by a person in consequence of the disclosure.  (4) If a person, when giving information to the Commission in response to a requirement of the Commission under this Part, claims that the information is confidential information, the Commission must, before disclosing the information otherwise than as referred to in subsection (2), give the person written notice of the proposed disclosure and the reasons for the disclosure.  (5) A person performing a function under this Act or a relevant industry regulation Act must not use confidential information for the purpose of securing a private benefit for himself or herself or for some other person.  (6) Information classified by the Commission as being confidential under subsection (1) is not liable to disclosure under the *Freedom of Information Act 1991*. | \* Nothing relevant | \* Nothing relevant |
| **Electricity Act 1996 (SA)** | **10—Technical Regulator's power to require information**  (1) The Technical Regulator may, by written notice, require a person to give the Technical Regulator, within a time stated in the notice (which must be reasonable), information in the person's possession that the Technical Regulator reasonably requires for the performance of the Technical Regulator's functions (whether under this Act or any other Act). | **11—Obligation to preserve confidentiality**  (1) The Technical Regulator must preserve the confidentiality of information gained by the Technical Regulator under this Act (including information gained by an authorized officer under Part 7) that—  (a) could affect the competitive position of an electricity entity or other person;  or  (b) is commercially sensitive for some other reason.  (1a) Despite subsection (1), the Technical Regulator may disclose confidential information in the following circumstances:  (a) as reasonably required in connection with the administration or enforcement of this Act (including to the Minister, the Commission and persons assisting the Commission) or as otherwise related to the performance of the Technical Regulator's functions (whether under this Act or any other Act);  (b) to a person concerned in the administration or enforcement of another law of the State, or a law of the Commonwealth or another State or a Territory of the Commonwealth, for purposes related to the administration or operation of that other law;  (c) to a government agency or instrumentality of this State, the Commonwealth or another State or Territory of the Commonwealth for purposes related to the performance of its functions (or to a person acting on behalf of such a government agency or instrumentality);  (d) with the consent of the person who gave the information or to whom the  information relates;  (e) as required by a court or tribunal constituted by law;  (f) as authorised by the Minister.  (2) Information classified by the Technical Regulator as confidential is not liable to disclosure under the *Freedom of Information Act 1991*. | **55I—Confidentiality of information**  (1) A person who gives the Technical Regulator information, or produces documents, may ask the Technical Regulator to keep the information or the contents of the documents confidential.  (2) The Technical Regulator may, after considering representations from the parties (or the other party), impose conditions limiting access to, or disclosure of, the information or documentary material in order—  (a) to consider in confidence information that has commercial value to a person  or relates to the commercial or financial affairs of a person (the Technical  Regulator being satisfied that it is reasonably foreseeable that public  disclosure of the information could cause significant damage to a person or the interests of a person or confer an unfair commercial or financial advantage on a person); or  (b) to ensure that the Technical Regulator does not—  (i) breach any law, order or direction of a court or tribunal constituted by law, or other legal obligation or duty; or  (ii) unreasonably expose himself or herself to any legal process or liability.  (3) A person must not contravene a condition imposed under subsection (2). | \* Nothing relevant |
| **National Electricity (South Australia) Act 1996** | **17—Provision of information and assistance by ESCoSA**  (1) Despite any other Act or law, ESCoSA is authorised, on its own initiative or at the request of the AER:  (a) to provide the AER with such information (including information given in confidence) in the possession or control of ESCoSA that is reasonably required by the AER for the purposes of this Part or the National Electricity Law; and  (b) to provide the AER with such other assistance as is reasonably required by the AER to perform or exercise a function or power under this Part or the National Electricity Law.  (2) Despite any other Act or law, ESCoSA may authorise the AER to disclose information provided under subsection (1) even if the information was given to ESCoSA in confidence.  (3) Nothing done, or authorised to be done, by ESCoSA in acting under subsection (1) or (2)—  (a) constitutes a breach of, or default under, an Act or other law; or  (b) constitutes a breach of, or default under, a contract, agreement, understanding or undertaking; or  (c) constitutes a breach of a duty of confidence (whether arising by contract, in equity or by custom) or in any other way; or  (d) constitutes a civil or criminal wrong; or  (e) terminates an agreement or obligation or fulfills any condition that allows a person to terminate an agreement or obligation, or gives rise to any other right or remedy; or  (f) releases a surety or any other obligee wholly or in part from an obligation. | \*Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **ETSA Utilities Electricity Distribution Licence** | \* Nothing relevant | 23. Confidentiality  23.1 The Licensee must, unless otherwise required by law, this licence an industry code or the National Electricity Rules:  (a) comply with any rules made by the Commission from time to time relating to the use of information acquired by the Licensee in the course of operating the business authorised by this licence; and  (b) ensure that information concerning a customer or any other person connected to the Licensee’s distribution network is not disclosed without the explicit informed consent of the customer or the other person connected to the Licensee’s distribution network.  23.2 The Licensee must not disclose confidential information to an intelligence or law enforcement agency unless requested to do so by an intelligence or law enforcement agency on the basis that:  (a) disclosure is necessary under the terms of a warrant issued under Division 2 of the Australian Security Intelligence Organisation Act 1979 or under the terms of any other court order; or  (b) disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty or for the protection of the public revenue; or  (c) disclosure is necessary to safeguard the national security of Australia.  23.3 The Licensee may accept an assertion of an intelligence or law enforcement agency, without making further enquiry, for the purposes of clause 23.2(b) and clause 23.2(c). | \* Nothing relevant | \* Nothing relevant |
| **Electricity Retail Authorisation (under the National Energy Retail Law).** | The AER website only lists the authorised retailers without including details of their authorisations.  The only publicly available information is the AER guidelines on assessing authorisation applications. A review of the guidelines for anything regarding data or information indicates that they don't say how an applicant should address issues regarding privacy and confidentiality. | | | |
| **Electricity (General) Regulations 2012 (SA)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | **20—Prescribed information in small customer accounts for purposes of section 24(2)(da) of Act**  For the purposes of section 24(2)(da) of the Act, the following provisions apply:  (a) the electricity entity must include in each account for electricity charges sent to a small customer for electricity supplythrough a particular metered connection point the following information:  (i) the customer's average daily consumption level, expressed in kWh, of electricity supplied through the connection point for the period to which the account relates;  (ii) the customer's average daily consumption level, expressed in kWh, of electricity supplied through the connection point for each period during the preceding 12 months in respect of which the customer was sent by the entity an account for electricity supply through the connection point; |
| **Electricity Metering Code (SA)** | ***4.3. Collection of Metering Data***  4.3.1. The person responsible for the *metering installation* must collect data stored in a *metering installation* by reading the *meter* at the *customer’s supply address* in accordance with this Chapter 4.  4.3.2. A *customer*may arrange with the person responsible for the *metering installation* or its *retailer* that the data stored in the *metering installation* be collected by the person responsible for the *metering installation*:  (a) by inspecting the *metering installation*;  (b) where the *metering installation* is capable of providing data by electronic means, by electronic means; or  (c) where the *metering installation* is capable of providing data by any other means, by any other means.  4.3.3. The person responsible for the *metering installation* may charge a *customer* for the collection of *metering data* under clause 4.3.2 to the extent that its costs of collection are higher than they would otherwise be.  4.3.4. The person responsible for the *metering installation* must use its *best endeavours* to ensure that *interval energy data* or *accumulated energy data* is:  (a) collected from all *metering installations* at least quarterly or, where a greater frequency has been agreed with a *customer* or a *customer’s retailer*, at that greater frequency; and  (b) collected from each manually read *metering installation* by means of an *actual meter reading* at least once in each 12 month period.  4.3.5. Where the person responsible:  (a) is required under clause 4.3.4 (a) to use its *best endeavours* to collect *interval energy data* or *accumulated energy data* from a *metering installation* at least quarterly; and  (b) has not obtained an *actual meter reading* in respect of that *metering installation* for three successive quarters by reason of the denial of access to the *metering installation* by the *customer*, then the person responsible must use its *best endeavours* to obtain an *actual meter reading* in respect of that *metering installation* for the subsequent quarter.  4.3.6. When *interval energy data* or *accumulated energy data* is not collected by a person responsible for the *metering installation* from a *metering installation* by way of an *actual meter reading* at the applicable meter reading frequency under clause 4.3.4(a), an *estimated* *read* must be obtained by the person responsible for the *metering* *installation*.  4.3.7. An *estimated read* obtained for the purposes of clause 4.3.5 must be provided to the *retailer* within 10 *business days* of the scheduled meter reading date under clause 4.3.4(a).  4.3.8. The person responsible for the *metering installation* must perform a *special meter read* at the request of a *customer* or a *customer’s retailer*.  4.3.9. The person responsible for the *metering installation* must perform a final read at the request of a *customer* or a *customer’s retailer*.  4.3.10. Where the *metering data* held in the *metering installation* is protected from direct or remote access by suitable password and security controls, such passwords and security controls must be used.  4.3.11 Passwords must be treated as confidential information in accordance with clause 5.4. | ***5.4. Confidentiality***  5.4.2. The *distributor*, the person responsible for the *metering installation* and *retailers*:  (a) must not disclose a *customer’s metering data* to any person except as permitted by this industry code, the *National Electricity* *Rules* or the *Metrology Procedure*;  (b) must only use or reproduce a *customer’s metering data* for the purpose for which it was collected under this industry code or another purpose contemplated by any other code, the *National* *Electricity Rules* or the *Metrology Procedure*;  (c) must not permit unauthorised persons to have access to a *customer’s metering data*;  (d) must not disclose a *customer’s metering data* to any person without the *explicit informed consent* of the *customer*; and  (e) must ensure that the *metering data* and other information obtained from a *customer* is treated in accordance with the *explicit informed consent* of the *customer* and in accordance with any *applicable regulatory instrument*.  5.4.3. This clause 5.4 does not prevent:  (a) the disclosure, use or reproduction of *metering data* if the *metering data* is at the time generally and publicly available otherwise then as a result of breach of confidence by the *distributor*, a person responsible for the *metering installation* or a *retailer* or its *disclosees*;  (b) the disclosure of *metering data* by the *distributor*, a person responsible for the *metering installation* or a *retailer* or its *disclosees* to:  (i) its employees or the employees of its related bodies corporate subject to any *applicable regulatory instrument*;  (ii) or its legal or other professional advisor, auditor or other consultant, requiring the *metering data* for the purposes of this industry code or any other code or for the purpose of advising the *distributor*, the person responsible for the *metering installation* or the *retailer* or *disclosee* in relation to those purposes;  (c) the disclosure, use or reproduction of *metering data* with the *explicit informed consent* of the relevant *customer*;  (d) the disclosure, use or reproduction of *metering data* to the extent required by law or by lawful requirement of:  (i) any government or governmental body, authority or agency having jurisdiction over the *distributor*, a person responsible for the *metering installation* or a *retailer* or its related  bodies corporate;  (ii) any stock exchange having jurisdiction over the *distributor*, a person responsible for the *metering installation* or a *retailer* or its *related bodies corporate*; or  (iii) the *Commission*;  (e) the disclosure, use or reproduction of *metering data* required in connection with legal proceedings, arbitration, expert determination or other dispute resolution mechanism under this industry code or any other code, the *National Electricity Rules* or the *Metrology Procedure*;  (f) the disclosure, use or reproduction of *metering data* which is trivial in nature;  (g) the disclosure use or reproduction of *metering data* required to protect the safety of personnel or equipment; or  (h) the disclosure use or reproduction of *metering data* by or on behalf of the *distributor*, the person responsible for the *metering* *installation* or a *retailer* to the extent it is reasonably required in connection with the *distributor*’s, the person responsible for the *metering installation*’s or the *retailer*’s financing arrangements, investment in the *distributor*, the person responsible for the *metering installation* or the *retailer* or disposal of the *distributor*, the person responsible for the *metering installation* or the *retailer*.  5.4.4. In the case of a disclosure under clause 5.4.3(b) and clause 5.4.3(h), the *distributor*, a person responsible for the *metering installation* or the *retailer* making the disclosure must inform the relevant *disclosee* of the confidentiality of the *metering data* and use reasonable endeavours to ensure that the *disclosee* keeps the *metering data* confidential. | ***5.4. Confidentiality***  5.4.1. The *distributor*, a person responsible for the *metering installation* and *retailers* must keep *metering data* confidential and use reasonable endeavours to protect and preserve the confidential nature of the *metering data* and must comply with any *applicable regulatory* *instrument*.  ***4.7. Storage of Metering Data***  4.7.1. The person responsible for the *metering installation* must store *metering data* in respect of each *metering installation* and *metering data* in respect of each unmetered *connection point*, for a period of 7years, in the form in which it was collected under clause 4.3 or calculated under clause 4.5. | ***4.6 Access to Metering Installation***  4.6.1 The person responsible for the metering installation must give a customer access to data stored in a metering installation used to measure and record the amount of electricity stored to its connection point, either by inspecting the metering installation or, where available, by electronic access to the metering installation.  4.6.2 The person responsible for the metering installation must, on request from a customer or a customer’s retailer provide the customer with access to the energy data and the metering data in respect of the metering installation which measures and records the amount of electricity supplied to the connection point of the customer.  ***4.8. Access to Metering Data***  4.8.1. The person responsible for the *metering installation* must ensure that access is provided to *metering data* (whether actual or substituted under clause 4.4 at the frequency agreed under clause 4.3.4(a)).  4.8.2. The format of *metering data* provided under clause 4.8.1 must be in accordance with Schedule 4 reference 1.8 of Part A of the *Metrology* *Procedure*, 4.8.3. For the purposes of this clause 4.8, all references in the *Metrology* *Procedure* to:  (a) a Financially Responsible Market Participant are references to a r*etailer*;  (b) “each *metering installation* for which the *financially responsible Market Participant* has registered with *AEMO*” in *Metrology Procedure* clause 3.8.1 are references to each *metering installation* associated with a *customer’s supply address*; and  (c) type 7 *metering installations* are references to unmetered *connection points*.  ***5.3. Access to data***  5.3.1. Where a *sample meter* has been installed at a *connection point* by the *distributor*, the person responsible for the *metering installation* must give a *customer* access to the data stored in that *sample meter* as *accumulated energy data* and not as *interval energy data*.  5.3.2. The person responsible for the *metering installation* must, on written request from a *customer*, provide facilities to enable the *customer* to access data stored in a *metering installation* by remote electronic means.  5.3.3. Where the person responsible for the *metering installation* has provided facilities to enable the *customer* to access data stored in a *metering installation* by remote electronic means, if remote electronic access to the *metering installation* is unavailable for a period of 5 consecutive *business days* due to the actions within the control of the person responsible for the *metering installation*, the person responsible for the *metering installation* must, if requested by the *customer*, obtain data locally from the *metering installation* and provide that data to the *customer* at the person responsible for the *metering installation*’s cost.  5.3.4. For *connection points* at which the *annual electricity consumption level* is less than 160MWh per annum, the *energy data* or *metering data* provided to the *customer* or the *customer’s retailer* must beprovided within the timeframes to enable a *retailer* to discharge itsminimum obligations under the *Energy Retail Code*. |
| **Electricity Distribution Code 2013 (SA)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Prepayment Meter System Code (SA)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | ***2.4. Provision of Information***  ***Consumption Information***  2.4.3. On request, a *retailer*must, at no charge, give a *small customer*the following information relating to the *small customer’s supply address*:  (a) total energy consumption;  (b) average daily consumption; and  (c) average daily cost of consumption for the previous two years or since the commencement of the *prepayment* *meter market contract*(which ever is the shorter) divided into quarterly segments.  ***4.3. System Requirements***  4.3.1. A *retailer* offering a *prepayment meter market contract* must ensure that:  ***Access to Metering Data***  (f) access is provided to *metering data* as required by all *applicable regulatory instruments* |

## NEW SOUTH WALES

Table D.3: Analysis of energy market regulatory instruments – New South Wales

| **Instrument** | **Collection of data** | **Use and disclosure of data** | **Data security (storage and protection)** | **Access to data** |
| --- | --- | --- | --- | --- |
| **Appendix F of the Compliance Reporting Manual for Electricity Retail Suppliers (**Electricity retail supplier licence conditions and obligations under licence conditions) | \* Nothing relevant | **Appendix sets out brief description of obligation:**  **Item Number 77**: Section 63D of the ESA and Clause 9.2.2(b) of the MOR  A retailer must not disclose a customer’s metering data, must only use or reproduce a customer’s metering data for the purpose for which it was collected, must not disclose or provide access to data to any person without the written consent of the customer and must ensure that the data and other information obtained from a customer is treated in accordance with the consent of the customer. | **Appendix sets out brief description of obligation:**  **Item Number 76:** Section 63D of the ESA and Clause 9.2.2(a) of the MOR  A retailer must keep metering data confidential and use reasonable endeavours to protect and preserve confidentiality  **Item Number 78:** Section 63D of the ESA and Clause 9.2.2(d) of the MOR  In the case of disclosure under clauses 9.2.2(c)(2) and 9.2.2(c)(8), the retailer making the disclosure must inform the disclosee of the confidentiality of the metering data and use reasonable endeavours to ensure that the disclose keeps the metering data confidential. | \* Nothing relevant |
| **Schedule Listing Ministerially imposed Licence Conditions for Distribution Network Service Providers** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Independent Pricing and Regulatory Tribunal Act 1992 (NSW)** | \*Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **National Electricity (New South Wales) Act 1997** | \*Nothing relevant | \*Nothing relevant | \*Nothing relevant | \*Nothing relevant |
| **Electricity Supply Act 1995 (NSW)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Electricity Supply (General) Regulations 2001 (NSW)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | **4**   **Contents of bill** (1)  This clause applies to the following customer contracts:  (a)  standard form customer contracts, (b)  negotiated customer contracts between licence holders and small retail customers.  (2)  The information to be included in a bill issued by the licence holder under a customer contract must include the following:  (f3)  if the bill was issued as a result of a meter reading, the values of the meter readings at the start and end of the billing period if:  (i)  the meter concerned measures and records consumption of energy on an accumulation basis only, or (ii)  the meter concerned measures and records consumption of electricity derived from interval metering data (within the meaning of the *National Electricity (NSW) Regulations*) and the required metering data is reasonably available,  (f4)  if the bill was issued as a result of an estimation, the values of the estimates at the start and end of the billing period,  **28**  **Provision of information about bills and related matters**  (1)  This clause applies to the following customer contracts:  (a)  standard form customer supply contracts,  (b)  negotiated customer supply contracts between suppliers and small retail customers.  (2)  The supplier must, if requested to do so by the customer, supply the following information to the customer within a reasonable time of receiving the request:  (b)  information about meter readings and meter registrations connected with a bill.  **31**   **Matters related to electricity consumption to be included in bill**  (1)  The information to be included in a bill issued by the supplier under a standard form customer supply contract must include the following:  (a)  the particulars of meter readings for the period, (b)  the estimated or measured quantity of electricity supplied in kilowatt hours, (d)  particulars of the quantity of electricity of each category supplied during the billing period or estimated to have been supplied during the period, (e)  particulars of the average daily consumption of all electricity supplied during the billing period in respect of that bill (expressed in kilowatt hours), (f)  if a bill was rendered by the same supplier for the corresponding billing period during the previous year, particulars of the average daily consumption during that previous billing period.  **33**   **Provision of historical billing information** (1)  A supplier must, if requested to do so by a small retail customer or former small retail customer, give to the customer copies of, or information about, previous bills issued by the supplier to the customer within a reasonable time of receiving the request.  (3)  The supplier may provide copies of bills, or billing information, to a person other than the small retail customer, only if the customer consents in writing to the provision of the bills or billing information to the other person. (4)  For the avoidance of doubt, this clause does not prevent a supplier from providing consumption information for the purposes of customer registration, customer transfer and wholesale settlement of payments in the national electricity market or for any other purpose that the supplier is legally required to do so. |
| **Market Operation Rules (NSW Rules for Electricity Metering) 2001** | **10.1.7 Collection of metering data**  (a) Subject to clause 10.1.7(b), a *first tier customer,* or a *Retailer* on behalf of a *first tier customer,* may arrange with an *LNSP* or a *Retailer* the manner in which data stored in *metering equipment* provided to the *first tier customer* is to be collected.  (b) A *first tier customer,* or a *Retailer* on behalf of a *first tier customer* may request that the data stored in *metering equipment* provided to it be collected by:  (1) an *LNSP*, by inspecting the *metering equipment*;  (2) an *LNSP*, by electronic means; or  (3) an *LNSP*, by any other means.  (c) An *LNSP* may charge a *first tier customer* for the collection of *metering data* under this clause 10.1.7 to the extent that its costs of collection arehigher than they would otherwise be. | **9.2.2 Confidentiality**  (b) An *LNSP*, a *Responsible Person* and a *Retailer*:  (1) must not disclose a *customer’s metering data* to any person except as permitted by this Market Operations Rule, the *Electricity Supply (General) Regulation 2001,* the *NEC* or the *Metrology Procedure*;  (2) must only use or reproduce a *customer’s metering data* for the purpose for which it was collected under this Market Operations Rule or another purpose contemplated by any other code under *The Act*, *Electricity Supply (General) Regulation 2001,* the *NEC* or the *Metrology Procedure*;  (3) must not disclose or provide access to a *customer’s metering data* to any person without the written consent of the *customer*; and  (4) must ensure that the *metering data* and other information obtained from a *customer* is treated in accordance with the consent of the *customer*.  (c) This clause 9.2.2 does not prevent:  (1) the disclosure, use or reproduction of *metering data* if the *metering data* is at the time generally and publicly available otherwise then as a result of breach of confidence by an *LNSP*, a *Responsible Person* or a *Retailer* or its *disclosees* ;  (2) the disclosure of *metering data* by an *LNSP*, a *Responsible Person* or a *Retailer* or its *disclosees* to:its employees or the employees of its *related bodies corporate*; orits legal or other professional advisor, auditor or other consultant, requiring the *metering data* for the purposes ofthis Market Operations Rule or any other code under *The Act* or for the purpose of advising the *LNSP*, the *Responsible Person* or the *Retailer* or *disclosee* (as the casemay be) in relation to those purposes;  (3) the disclosure, use or reproduction of *metering data* with the written consent of the relevant *customer*;  (4) the disclosure, use or reproduction of *metering data* to the extent required by law or by lawful requirement of: any government or governmental body, authority or agency having jurisdiction over an *LNSP*, a *Responsible Person* or a *Retailer* or its *related bodies corporate*; any stock exchange having jurisdiction over an *LNSP*, a *Responsible Person* or a *Retailer* or its *related bodies corporate*; or *IPART*.  (5) the disclosure, use or reproduction of *metering data* required in connection with legal proceedings, arbitration, expert determination or other dispute resolution mechanism under this Market Operations Rule or any other code under *The Act*, the *NEC* or the *Metrology Procedure*;  (6) the disclosure, use or reproduction of aggregated *metering data* by whole *customer* classes only;  (7) the disclosure use or reproduction of *metering data* required to protect the safety of personnel or equipment or to prevent a serious and imminent threat to any person’s life or health; or  (8) the disclosure use or reproduction of *metering data* by or on behalf of an *LNSP*, the *Responsible Person* or a *Retailer* to the extent it is reasonably required in connection with the *LNSP’s*, the *Responsible Person’s* or the *Retailer’s* financing arrangements, investment in the *LNSP*, the *Responsible* *Person* or the *Retailer* or disposal of the *LNSP*, the *Responsible Person* or the *Retailer*.  (d) In the case of a disclosure under clauses 9.2.2(c)(2) and 9.2.2(c)(8), the *LNSP*, a *Responsible Person* or the *Retailer* making the disclosure must inform the relevant *disclosee* of the confidentiality of the *metering data* and use *reasonable endeavours* to ensure that the *disclosee* keeps the *metering data* confidential. | **9.2.2 Confidentiality**  (a) An *LNSP*, a *Responsible Person* and a *Retailer* must keep *metering data* confidential and use *reasonable endeavours* to protect and preserve theconfidential nature of the *metering data;*  **10.1.8 Data security**  (a) Where the *energy data* held in the *metering equipment* is protected from direct or remote access by suitable password and security controls, such passwords and security controls must be used.  (b) An *LNSP* must treat passwords as confidential information in accordance with clause 9.2.2.  (c) The *customer* may only hold ‘read only’ passwords.  (d) The *LNSP* will hold ‘read only’ and ‘write’ passwords.  **10.5 Storage of energy data**  An *LNSP* must store *energy data* in respect of separate *metering equipment* and unmetered *loads* separately, for a period of 7 years, in the form in which it was collected under clause 10.1. | **9.2 Information**  **9.2.1 Access to data**  (a) A *customer* is entitled to access data stored in *metering equipment* used to measure and record the amount of electricity *supplied* to its *electrical* *installation*, either by inspecting the *metering equipment* or, where available, by electronic access to the *metering equipment*.  (b) Subject to clause 9.2.1(c), an *LNSP* or a *Responsible Person* (as the case may be) must, on written request from a *customer* or a *Retailer* on behalf of a *customer*, provide facilities to enable the *customer* to electronically access data stored in *metering equipment,* where electronic data is available, provided by the *LNSP* or the *Responsible* *Person*.  (c) A *customer* who accesses data stored in *metering equipment* by remote electronic means must compensate the *LNSP* or the *Responsible Person* (as the case may be), for any cost incurred by the latter as a result of that access.  (d) Where an *LNSP* or a *Responsible Person* has provided facilities to enable the *customer* to electronically access data stored in *metering* *equipment*, if remote electronic access to *metering equipment* is unavailable for a period of five consecutive *business days* due to the actions within the control of the *LNSP* or the *Responsible Person* (as the case may be), the *LNSP* or the *Responsible Person* must, if requested by the *customer* or a *Retailer* on behalf of a *customer*, obtain data locally from the *metering equipment* and provide that data to the *customer* at the *LNSP’s* or the *Responsible Person’s* cost.  (e) Subject to clause 9.2.1(f), an *LNSP* or a *Responsible Person* (as the case may be) must, on request from a *customer* or a *customer’s Retailer*, provide the *customer* with access to the *energy data* and the *metering* *data* in respect of the *metering equipment* which measures and records the amount of electricity supplied to the *electrical installation* of the *customer*.  **10.6 Access to energy data**  An *LNSP* must ensure that access is provided to *energy data* in accordance with clauses 3.7.1 and 3.7.4 of the *Metrology Procedure*. For the purposes of this clause, all references in the *Metrology Procedure* to:  (a) a *Responsible Person* are references to an *LNSP*;  (b) a Financially Responsible Market Participant are references to a *Retailer*;  (c) “each metering installation for which the Financially Responsible Market Participant was registered with *NEMMCO*” in clause 3.7.1 are reference to each *metering installation* associated with a *customer’s connection point*;  (d) type 5 or type 6 *metering installation* are references to *interval metering equipment* and *accumulation metering equipment* respectively; and  (e) a reference to a type 7 *metering installation* are references to an unmetered *load*. |
| **Energy Marketing Code of Conduct** | \*Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Market Operations (NSW Transfer Rules for Retail Electricity Supply) Rule No. 4 of 2009** | \*Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Schedule Listing Ministerially imposed Licence Conditions for Electricity Retail Service Providers** | \*Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |

## QUEENSLAND

Table D.4: Analysis of energy market regulatory instruments - Queensland

| **Instrument** | **Collection of data** | **Use and disclosure of data** | **Data security (storage and protection)** | **Access to data** |
| --- | --- | --- | --- | --- |
| **Electricity Act 1994 (Qld)** | **135G Regulator’s power to require documents or information**  (1) The regulator may, by notice, require a party to the dispute to give the regulator a stated document or information the regulator reasonably requires to decide who is the liable person.  (2) The notice must be accompanied by, or include, an information notice about the decision to make the requirement.  (3) The document or information must be given within a reasonable period after giving the notice, unless the party has a reasonable excuse.  (4) It is not a reasonable excuse not to give the document or information because it is confidential or because the party has agreed with another party or someone else not to give it to anyone else. | \* Nothing relevant | **135GA Regulator may require confidentiality to be observed**  (1) A person who gives the regulator information, or produces a document, may ask the regulator to keep the information or the contents of the document confidential.  (2) After considering representations from the parties to the dispute, the regulator may impose conditions limiting access to, or disclosure of, the information or document. *Example of a condition that may be imposed*— a condition that the parties, or a stated party, may use the information or document only for the mediation  (3) A person to whom a condition under subsection (2) applies must comply with the condition. | \* Nothing relevant |
| **Queensland Competition Authority Act 1997** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Pro forma Retail Authority with a retail area or without a retail area** | \* Nothing relevant  Note: conditions contained in legislation and regulations – individual licences can only be viewed with permission of holder and may contain additional terms to that contained in the pro forma licences. | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Pro forma Distribution Authority** | \* Nothing relevant  Note: conditions contained in legislation and regulations – individual licences can only be viewed with permission of holder and may contain additional terms to that contained in the pro forma licences. | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Electricity Regulation 2006 (Qld)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Annexure B to the Electricity Industry Code (Standard Retail Contract) (for a small customer who has not signed a Negotiated Retail Contract)** | \* Nothing relevant | **19 Privacy and Confidentiality**  **19.1 Privacy of Information**  Subject to clauses 19.2 and 23 of this contract, we must keep your information about you confidential in accordance with the *Privacy Act 1988* (Cth)   * 1. **Disclosure**   We may, however, disclose information about you:   1. if required or permitted by law to do so; 2. if we are required or permitted by our *retail authority* to do so, such as to a law enforcement agency; 3. where you give us written consent; 4. to your *distribution entity* or a metering provider to the extent that the information is for the purposes of arranging *customer connection services* or reading a meter; or 5. where it is necessary in order to obtain a credit check of your credit history   Clause 23 concerns the provision of the customer’s name, billing address and NMI to an electricity entity appointed as the retail entity of last resort. | \* Nothing relevant | \* Nothing relevant |
| **Electricity Industry Code (Qld)** | Chapter 9, Metering, applies to type 1 to 7 metering installations that are not covered by the National Electricity Rules, being connection points where the customer for the relevant premises is, or is taken to be, an excluded customer under the Electricity Act. An excluded customer is a small customer whose premises are connected, or to be connected, to a distribution entity’s supply network that is not connected to the national grid.  This table does not explore Chapter 9 on the basis that smart meters will not be installed for excluded customers. | | | **3.2** **Customer Information**  **3.2.1 Provision of information**  A *distribution entity* must, on request by a customer or a customer’s *retail entity*, provide information about the customer’s energy consumption or the distribution entity’s charges, but information requested more than once in any 12 month period may be provided subject to a reasonable charge. |

## AUSTRALIAN CAPITAL TERRITORY

Table D.5: Analysis of energy market regulatory instruments – Australian Capital Territory

| **Instrument** | **Collection of data** | **Use and disclosure of data** | **Data security (storage and protection)** | **Access to data** |
| --- | --- | --- | --- | --- |
| **Utilities Act 2000 (ACT)** | \* Nothing relevant | \* Nothing relevant | **51 Protection of personal information**  (1) In this section:  ***Information Privacy Principles*** means the Information Privacy Principles under the *Privacy Act 1988* (Cwlth, s 6), other than Principle 5, clause 4 (b).  (2) This section applies to personal information gained by a utility in relation to the provision of a utility service.  (3) A utility must deal with personal information in accordance with the Information Privacy Principles as if it were a prescribed authority, within the meaning of the *Freedom of Information Act 1989*, to which the *Privacy Act 1988* (Cwlth) applies. | \* Nothing relevant |
| **Independent Competition and Regulatory Commission Act 1997 (ACT)** | **41 Provision of information to commission**  (1) If the commission has reason to believe that a person has information or a document that may assist it in exercising its functions, it may, by written notice, require the person to give it the information or a copy of the document.  (2) A requirement must—  (a) identify the information or document; and  (b) specify the period within which the requirement is to be complied with; and  (c) specify the form in which the information or the copy of the document is to be given to the commission; and  (d) state that it is made under this section; and  (e) be accompanied by a copy of this part.  (3) The commission may also require a NERL retailer required to comply with the *Utilities Act 2000*—  (a) to conduct an audit, in a way approved by the commission, of the NERL retailer’s compliance with that Act; and  (b) to report the results of the audit to the commission.  (4) A person must not, without reasonable excuse, fail to comply with a requirement under this section. | **44 Confidential information—disclosure by commissioners and staff**  (1) A person must not disclose any confidential information obtained in carrying out the person’s functions in relation to this Act, except in accordance with subsection (3).  (2) A person must not use any confidential information obtained in carrying out the person’s functions in relation to this Act to obtain, directly or indirectly, a pecuniary or other advantage for himself or herself or any other person, except in accordance with subsection (3).  (3) A person may disclose or use confidential information if—  (a) the disclosure or use is made in the exercise of a function in relation to this Act or any other law of the Territory permitting the disclosure or use; or  (b) the disclosure or use is made with the consent of the person who supplied the information; or  (c) the disclosure or use is made in a legal proceeding at the direction of a court; or  (d) the information is in the public domain at the time that it is disclosed. | **45 Confidential information**—**notice of proposed disclosure**  (1) If the commission proposes to disclose confidential information under section 46, it must first give any affected person written notice inviting the person to show cause within 28 days after the date the notice is given why the confidential information should not be disclosed.  (2) A notice under subsection (1) must contain—  (a) particulars of the proposed disclosure, including details of the person or people to whom the confidential information is to be disclosed; and  (b) particulars of the facts and circumstances relied on by the commission to justify the disclosure; and  (c) a copy of the disclosure guidelines under section 46; and  (d) a statement to the effect that the affected person may, within 28 days after the day the notice is given, give the commission particulars of the facts and circumstances relied on to show cause why the proposed disclosure ought not to be carried out.  (3) In this section:  ***affected person*** means—  (a) the supplier of the confidential information to the commission; or  (b) anyone who provided the confidential information to the supplier, if the commission is aware of the identity and address of that person.  **46 Confidential information—general disclosure**  (1) Subject to section 47, the commission must only disclose confidential information if—  (a) it considers that, taking into account the disclosure guidelines under subsection (4)—  (i) the disclosure would not cause detriment to any person; or  (ii) although the disclosure would cause detriment to a person, the public benefit in disclosure outweighs the detriment; and  (c) it gives a notice to show cause in relation to the information or document under section 45; and  (d) 28 days have elapsed since the notice was given.  (2) In making a decision under subsection (1), the commission must take into account any representation made in accordance with the invitation in the notice under section 45.  (3) For this section, the disclosure of anything that is in the public domain at the time the commission proposes to disclose it is not taken to cause detriment to any person mentioned in subsection (1) (a) or (b).  **23 Confidential material in reports**  (1) If a final report or a special report includes protected confidential information, the commission must divide the report into 2 documents, as follows:  (a) a document (the ***sealed section***) containing the confidential information, or part of that information;  (b) a document (the ***unsealed section***) containing the rest of the report.  (2) If the commission divides a report, the commission must include in the unsealed section—  (a) a statement to the effect that there is a sealed section of the report including protected confidential information; and  (b) a general description of the contents of the sealed section.  (3) In this section: ***protected confidential information*** means confidential information the commission does not have the power to disclose under section 46 or under any law of the Territory other than this Act. | \* Nothing relevant |
| **ActewAGL Distribution Licence** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| **Electricity Retail Authorisation (under the National Energy Retail Law)** | The AER website only lists the authorised retailers without including details of their authorisations.  The only publicly available information is the AER guidelines on assessing authorisation applications. A review of the guidelines for anything regarding data or information indicates that they don't say how an applicant should address issues regarding privacy and confidentiality. | | | |
| **Electricity Feed-In Code 2012, Schedule 4, Applicability of Consumer Protection Code** | \* Nothing relevant | **7.3 Disclosure of Occupier information by an Electricity Distributor****or NERL retailer to a third party**  An Electricity distributor or NERL retailer must not disclose personal information about an Occupier to a third party except in accordance with the*Privacy Act 1988* (Cth) and the *Utilities Act 2000* (ACT). “Personal information”is defined in the *Privacy Act 1988* (Cth), section 6(1). | \* Nothing relevant | **7 Provision of information**  **7.1 Utility to provide information**  (1) An Electricity distributor or NERL retailer must, on request, provide an Occupier with information about the services provided by the Electricity distributor or NERL retailer to the Occupier Premises;  (2) An Electricity distributor or NERL retailer must, on request, provide an Occupier with information about:  (b) meter readings for Utility Services provided to the Occupier’s Premises by the Electricity distributor or NERL retailer; |

## TASMANIA

Table D.6: Analysis of energy market regulatory instruments – Tasmania

| **Instrument** | **Collection of data** | **Use and disclosure of data** | **Data security (storage and protection)** | **Access to data** |
| --- | --- | --- | --- | --- |
| **Electricity Supply Industry Act 1995** | **15. Regulator's power to require information**  (1) The Regulator may, by written notice, require a person to give the Regulator, within a time stated in the notice (which must be reasonable), information in the person's possession that the Regulator reasonably requires for the administration of this Act, the regulations, the Code and the National Electricity Rules.  (2) A person required to give information under this section must provide the information within the time stated in the notice.  (3) A person may not be compelled to give information under this section if the information might tend to incriminate the person of an offence. (4) A requirement to provide information under this section is not reviewable. | \* Nothing relevant | **16. Obligation to preserve confidentiality**  (1) The Regulator must preserve the confidentiality of information that –  (a) could affect the competitive position of an electricity entity or other person; or (b) is commercially sensitive for some other reason. (2) Information classified by the Regulator as confidential is not liable to disclosure under the [*Right to Information Act 2009*](http://www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_id=70%2B%2B2009%2BGS1%40EN%2B20130225000000;histon=;prompt=;rec=;term=).  (3) A classification of information by the Regulator as confidential (or not confidential) is not reviewable. | \* Nothing relevant |
| ***Electricity Supply Industry Distribution Licence***  *Aurora Energy Pty Ltd* | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| ***Electricity Retail Authorisation (under the National Energy Retail Law).*** | The AER website only lists the authorised retailers without including details of their authorisations.  The only publicly available information is the AER guidelines on assessing authorisation applications. A review of the guidelines for anything regarding data or information indicates that they don't say how an applicant should address issues regarding privacy and confidentiality. | | | |
| ***Electricity Supply Industry (Customer) Regulations* 2012** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| [***Electricity Supply Industry (Network Performance Requirements) Regulations* 2007 (TAS)**](http://www.thelaw.tas.gov.au/tocview/content.w3p;doc_id=+114+2007+AT@EN+20130225000000;rec=0) | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| ***Electricity Supply Industry (Price Control and Related Matters) Regulations* 2012 (TAS)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |
| ***Electricity Supply Industry Regulations* 2008 (TAS)** | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant | \* Nothing relevant |