



GUIDELINE NO. 10

CONFIDENTIALITY AND INFORMED CONSENT

ELECTRICITY AND GAS

MAY 2002

Enquiries concerning the currency of these Guideline should be addressed to -

Essential Services Commission
Level 2, 35 Spring Street
Melbourne Vic 3000

Telephone (03) 9651 0222 or Facsimile (03) 9651 3688

Email: reception@esc.vic.gov.au

Web site: <http://www.esc.vic.gov.au/>

Part	Issue No.	Date	Pages	Checked

PREFACE

The purpose of this guideline is to give guidance to retailers on two separate customer issues for retail competition in the electricity and gas industries: use and disclosure of customer information, and explicit informed consent for contracts.

The rationale for the requirements in this guideline is set out, in detail, in the Commission's decision of January 2002¹. It can be seen from that decision that the Commission considered that, having regard to its objectives, it was inappropriate for it to impose on regulated entities a discrete regime relating to privacy issues, given the *Private Sector Privacy Act*². Nevertheless, it was also considered that:

- retailers should be treated equally in terms of privacy requirements, irrespective of whether they were "organisations" bound by the *Privacy Act*,
- customers should be entitled to equal levels of privacy protection, irrespective of their level of usage of electricity or gas; and
- the use and disclosure provisions of the privacy regime should apply to customer information, whenever collected, given that retailers were, under Victorian regulatory arrangements, required to observe certain privacy requirements concerning use and disclosure before commencement of the *Privacy Act*.

Part II of the guideline sets out in general terms the requirements which must be observed by licensees in complying with the National Privacy Principles which arise from the *Privacy Act*. A major purpose of this guideline is to outline the Commission's understanding of how those general terms apply in particular contexts. This is designed to help retailers to gain a better understanding of the Commission's view of the nature and extent of their responsibilities under their respective retail licences.

Given the desire not to establish a discrete privacy regime, but essentially to rely on the regime generally applicable to the private sector under the *Privacy Act*, the Commission has consulted extensively with the Office of the Federal Privacy Commissioner (OFPC). Many of the views expressed in this guideline reflect the Commission's understanding of advice and commentary of, and guidelines issued by, the OFPC³. However those views are irrelevant to the issue of whether the retailer is observing the *Privacy Act* and should not be relied on by a retailer when considering that issue.

Part II of the guideline (clauses 2.1.1 and 2.2.2) differentiates between customers who are natural persons and customers who are bodies corporate. The rationale for splitting the requirements is that the NPPs do not apply in relation to information about bodies corporate and therefore it was considered that a single requirement which applies the NPPs to all types of customers would create an inappropriate perception about the NPPs.

¹ See **Final Decision: Confidentiality and Informed Consent** on www.esc.vic.gov.au

² Victorian electricity and gas utilities were bound by the *Private Sector Privacy Act* from 21 December 2001.

³ The Commission will be establishing a Memorandum of Understanding with the OFPC to maintain consistency in approach and interpretation.

It was also considered, however, that customers who are bodies corporate should continue to enjoy some level of privacy protection, as they currently do, as long as the imposition of a discrete requirement relating to such customers could occur without creating undue complexity. The guideline therefore imposes use, disclosure and access responsibilities in relation to customers who are not natural persons (bodies corporate) which match the use, disclosure and access responsibilities that apply in relation to customers who are natural persons. Not all information about bodies corporate need be protected, however; only information obtained by an electricity or gas retailer in the ordinary course of its business.

Part III provides guidance on the requirement to ensure that explicit informed consent is received when customers enter market contracts or standing offer contracts which are not consistent with the Retail Code. The Commission considers that consent in these circumstances must be explicit (that is, “opt-in” consent). It is not considered appropriate that consent can be implied.

GUIDELINE NO. 10 – CONFIDENTIALITY AND INFORMED CONSENT

CONTENTS

Page

PART 1 INTRODUCTION

1	INTRODUCTION.....	1
1.1	Commencement of this guideline.....	1
1.2	Purpose and authority.....	1
1.3	Relationship with Other Requirements	1
1.4	Process for Revision.....	2
1.5	Copies of this guideline.....	2
2	GENERAL REQUIREMENT.....	3
2.1	Requirement.....	3
3	USE AND DISCLOSURE OF CUSTOMER INFORMATION.....	4
3.1	Relevant NPP	4
3.2	Primary Purpose.....	4
3.3	Related and Expected Exception.....	4
3.4	Consent.....	5
3.5	Direct Marketing	6
3.6	Legally Required or Authorised.....	7
4	WHEN EXPLICIT INFORMED CONSENT IS REQUIRED.....	7
4.1	Entering into a <i>contract</i>	7
4.2	Estimated bills and different billing cycles.....	8
4.3	Scope of this Part 3	8
5	REQUIREMENTS FOR CONSENT TO BE EXPLICIT AND INFORMED.....	8
5.1	General Requirements	8
5.2	Explicit consent	8
5.3	Consent must be informed.....	9
5.4	Competence and capacity	9
6	RECORD KEEPING.....	9
6.1	<i>Explicit informed consent</i> must be verifiable and auditable	9
6.2	Access	10
7	GLOSSARY.....	10
7.1	General.....	12
	ATTACHMENT: THE NATIONAL PRIVACY PRINCIPLES	13

PART 1 INTRODUCTION

1 INTRODUCTION

1.1 Commencement of this guideline

This guideline applies on and from 1 July 2002 for licensed electricity retailers and on and from 1 October 2002 for licensed gas retailers.

1.2 Purpose and authority

The purpose of this guideline is to give guidance to retailers on two separate customer issues for retail competition in the electricity and gas industries: use and disclosure of customer information, and explicit informed consent for contracts. These issues are covered in Parts II and III respectively. Each of these Parts can be read independently from the other.

Use and disclosure of customer information

1.2.1 Each *Retail Code* obliges *retailers* to comply with any relevant industry guideline concerning the use or disclosure of personal information about a *customer*.⁴

1.2.2 In addition, under its *retail licence*, each electricity *retailer*⁵ is bound to comply with any guideline concerning the use or disclosure of personal information about a customer. The scope of this requirement extends beyond *relevant customers* to any other *customers*.

Explicit Informed Consent for contracts

1.2.3 Part 1 of schedule 1 of each *retailer's retail licence* and Attachment 1 of the *Gas Retail Rules* defines "*explicit informed consent*" to have the meaning given to that term by any applicable guideline.

1.2.4 This guideline defines "*explicit informed consent*" for the purposes of the *retailers' retail licences*, the *Retail Codes* and the *Gas Retail Rules*.

1.3 Relationship with Other Requirements

1.3.1 From the date of its application, this guideline takes the place of the interim guidelines issued by the Office of the Regulator-General, Victoria⁶ with respect to the electricity and gas industries.

⁴ See clause 29 of the Electricity *Retail Code* and, from 2 July 2002, clause 29 of the Gas *Retail Code* (currently clause 21 of the Gas *Retail Code*).

⁵ Consultation will occur shortly on proposed amendments to the gas *retail* licenses to ensure consistency.

⁶ The Office of the Regulator-General, Victoria became the Essential Services Commission on 1 January 2002.

1.3.2 The *Commission* does not intend that this guideline exclude, limit or qualify the nature or extent of any obligation or liability of a *retailer* arising other than in respect of this guideline, including any obligation or liability arising:

- under any condition of a *retail licence* (other than the condition requiring compliance with this guideline);
- in relation to ring-fencing or credit management requirements;
- under any law (including the *Privacy Act*).

1.3.3 In this guideline the *Commission* expresses views as to the interpretation of certain of the *NPPs*, in particular contexts. While those views may be relevant as to whether a *retailer* is complying with its *retail licence* provision (to the extent indicated in section 2), those views are irrelevant as to whether the *retailer* is observing the *Privacy Act*, and should not be relied on by a *retailer* when considering that issue.

1.3.4 Many of the views expressed in this guideline reflect the *Commission's* understanding of advice and commentary of, and guidelines issued by, the Office of the Federal Privacy Commissioner. However, nothing in this guideline should be taken as a guide to the way in which the Office of the Federal Privacy Commissioner would perform and exercise its duties and powers in any particular circumstances.

1.4 Process for Revision

1.4.1 The *Commission* may amend the guideline for the purposes of its application under the *retail licence* and also for the purposes of its application otherwise than under the licence.

1.4.2 The *Commission* will notify *retailers* of the amendment and the date on which it is to take effect.

1.4.3 In addition, unless the *Commission* considers (having regard to its objectives under the relevant *Industry Act*) that the amendment is urgent, the *Commission* will only give notice of an amendment after having:

- sought input from industry participants, consumer representatives and other interested parties;
- published a draft of an amendment for comment by industry participants and other interested parties;
- had regard to any such comments prior to giving notice of the amendment.

1.5 Copies of this guideline

Each *retailer* must:

- (a) publish a copy of this guideline on its web-site; and
- (b) give a copy of this guideline to any person, on request by that person.

PART 2 CONFIDENTIALITY

2 GENERAL REQUIREMENT

2.1 Requirement

2.1.1 Each *retailer* must not *breach* any *NPP* on or after the date that this guideline applies:

- even if the *retailer* is not an organisation under the *Privacy Act*;
- as if each of *NPPs* 2.1, 2.2, 2.3 and 6 applied in relation to *customer information* whenever collected (including *customer information* collected prior to commencement of the *Privacy Sector Privacy Act* or prior to the date on and from which this guideline applies);
- as if each reference in the *NPPs* (and in relevant *Privacy Act* definitions) to personal information were a reference to *customer information*;
- subject to the above, as if at any particular time the nature and extent of the obligations and requirements under each *NPP* were assessed by reference to (in order of priority):
 - first, judicial decisions on or in relation to the *NPP* made prior to that time;
 - secondly, guidelines of the Office of the Federal Privacy Commissioner issued prior to that time; and
 - thirdly, any *Commission* interpretation of the *NPP* as reflected in this guideline.

2.1.2 Each *retailer* must:

- not, on or after the date that this guideline applies, use or disclose *corporate client information* except insofar as the information could be used or disclosed without contravening the requirement outlined in clause 2.1.1; and
- on and after the date that this guideline applies, provide each of its *corporate clients* with access to *corporate client information* held by the retailer about the *corporate client* on request by the *corporate client*, except to the extent that a failure to provide such access would not contravene the requirement outlined in clause 2.1.1.

as if the relevant *corporate client* were an individual and the *corporate client information* is *customer information*.

3 USE AND DISCLOSURE OF CUSTOMER INFORMATION

3.1 Relevant NPP

Under *NPPs*, 2.1, 2.2 and 2.3 a *retailer* must not use or disclose *customer information* about a *customer* for a purpose other than the primary purpose of collection unless, amongst other things:

- the relevant purpose is related to the primary purpose of collection and the *customer* would reasonably expect the *retailer* to use or disclose the information for the relevant purpose; or⁷
- the *customer* has consented to the use or disclosure; or
- (in terms of use of *customer information*) the relevant purpose is direct marketing and, amongst other things, it is impracticable for the *retailer* to seek the *customer's* consent before that use of the information; or
- the use or disclosure is required or authorised by or under law.

3.2 Primary Purpose

3.2.1 A *retailer* may use or disclose *customer information* about a *customer* for the primary purpose of collection of the information.

3.2.2 The *Commission* interprets this as allowing the use and disclosure of *customer information* by a *retailer* if the purpose of the use or disclosure is to provide the core, underlying, service which the *customer* has contracted with the *retailer* to provide (or proposes to contract with the *retailer* to provide).

3.2.3 Accordingly, if a *retailer* has contracted with a *customer* to sell electricity to the *customer*, the *retailer* may only use or disclose *customer information* about the *customer* for the purpose of providing electricity under the contract.⁸

3.3 Related and Expected Exception

3.3.1 A *retailer* might use or disclose *customer information* about a customer for a purpose which is related to the primary purpose of collection where the *customer* would reasonably expect the *retailer* to use or disclose the information for the relevant purpose.

3.3.2 The *Commission* interprets this as allowing use and disclosure of *customer information* for the purposes of marketing activities that arise out of the nature of the contract which the *retailer* has with the *customer* concerned (or which the *customer* concerned proposes to make with the *retailer*).

⁷ This assumes the information of concern is not sensitive information, for the purposes of the *Privacy Act*.

⁸ Note that neither the Commission nor the Office of the Federal Privacy Commissioner are implying that other material cannot be marketed to *customers* if a *customer's* consent is received – see clause 3.4 as to whether this consent should be explicit or implied.

- 3.3.3 For example, if a *retailer* has a contract with a *customer* under which the *retailer* sells gas to the *customer*, the *Commission* interprets this exception as allowing the *retailer* to use and disclose *customer information* about the *customer* for the purpose of marketing gas supply services to the *customer*. This exception would not, however, allow the use and disclosure of *customer* information for the marketing of electricity supply services to that *customer* unless explicit or implied consent, in accordance with this guideline, has been given by the *customer*.
- 3.3.4 The *Commission* further interprets this exception to apply if *customer information* is used by a *retailer* for conducting customer surveys.

3.4 Consent

- 3.4.1 A *retailer* might use or disclose *customer information* about a *customer* for a purpose if the *customer* has consented to that use or disclosure.
- 3.4.2 The *Commission* interprets the *NPPs* as allowing use of *customer information* for the purpose of seeking consent to any particular use or disclosure of the information. Further, as a *retailer* may disclose information to a related body corporate (see clause 3.6.2), this related body corporate may then seek consent from the *customer* to market its particular services to that *customer*.
- 3.4.3 If customer consent is required for *customer information* to be used or disclosed, the *Commission* considers that the relevant consent must be given by a person competent to give it, and must be informed.
- 3.4.4 If it can be established that a person has given consent, the *Commission* would generally be prepared to assume that the person was competent to do so. However, in general, in order for an individual to be competent to give consent, the individual must be capable of understanding issues, forming views based on reasoned judgement and communicating his or her decision. In order for a person to be competent to give consent on behalf of an individual, the person must have legal authority to do so.
- 3.4.5 It is inherent in any claim that a person has consented to something that the person knows what they have consented to.
- 3.4.6 The *Commission* will assume the requisite knowledge in relation to a consent if the circumstances are such to suggest that the consent was informed. The chances of a *customer's* consent being considered to have been informed are:
- reduced the more obscure (or the less precise) the description of both the relevant use or disclosure and the consequences, if any, for the *customer* of consenting to that use or disclosure; and
 - increased the more clear it is that the *customer* would have been aware, when providing consent, what the particular use or disclosure was intended to be. For example, if a *customer* has been fully and adequately informed, in plain English, of all matters relevant to the provision of his, her or its consent and the particular use or disclosure concerned was specifically dealt with by those matters, it is highly likely that any "consent" to the use or disclosure would be considered to have been informed.

3.4.7 Consent may be explicit or implied. Where consent is explicit, this is consent given:

- in *writing* signed by the *customer*;
- by *electronic communication* signed by the *customer*; or
- verbally.

3.4.8 While consent may be implied, the circumstances in which the *Commission* will consider that consent has been given implicitly are limited. In particular, it must be reasonable to infer from the circumstances (and, in particular, the conduct of the *customer* and *retailer* concerned) that informed consent has been provided to the particular use or disclosure.

3.4.9 For example, in certain circumstances, a failure of a *customer* to "opt-out" might be considered to constitute implied consent. Whether a failure to opt-out constitutes implied consent depends on all relevant circumstances. In this regard, the *Commission* considers that:

- the more serious the consequences for the *customer* concerned of the relevant use or disclosure the less likely it is that the implied consent would be considered to have been given. For example, the *Commission* views disclosure of *customer information* to a third party marketer as relatively serious, when compared to use of *customer information* by a *retailer* to market its own energy related services;
- the more obscure the opt out election from the perspective of the *customer* concerned, or the more difficult it is for the *customer* to make that election, the less likely it is that implied consent would be considered to have been given. The reverse, however, applies if the opt out election is prominently displayed in material where it may be reasonable to conclude that the opt out election would have been examined by the *customer* concerned, and the *customer* is easily able to exercise the "opt-out" option;
- it is unlikely that consent to receive marketing material on-line could be implied from a failure to object to receiving it in that form (unless, possibly, that failure occurs in the context of an existing on-line relationship).

3.5 Direct Marketing

3.5.1 A *retailer* might use (but not disclose) *customer information* about a *customer* for the purpose of direct marketing if (amongst other things) it is impracticable for the *retailer* to seek the customer's consent before that use of the information.

3.5.2 The *Commission* considers that the test of impracticability is one that should be assessed by reference to applicable circumstances.

3.5.3 Nevertheless, as a general rule and noting that *retailers* are in regular contact with their *customers*, the *Commission* does not consider it would be impracticable for a *retailer* to seek the consent of a *customer* before using *customer information* about the *customer* for the purpose of direct marketing.

3.6 Legally Required or Authorised

3.6.1 A *retailer* might use or disclose *customer information* about a *customer* where the use or disclosure is required or authorised by or under law.

3.6.2 Under the *Privacy Act* disclosure of *customer information* by a *retailer* to a related body corporate of the *retailer* is permitted. A related body corporate to whom information is disclosed, however, will be deemed to have collected the relevant information for the primary purpose for which the *retailer* collected the information.

3.6.3 This exception to the general restriction on use and disclosure of *customer information* does not extend beyond related bodies corporate to encompass broader relationships established by contract (such as alliances).

3.6.4 Disclosure and use of customer credit information may also be permitted under Part IIIA of the *Privacy Act* if a *retailer* is a "credit provider" (noting, however, that use and disclosure of *customer information* in this situation might, in particular, be affected by the *Credit Management Guideline*).

3.6.5 Another example of the application of the legally permitted or authorised exception applies to an Order in Council made under an *Industry Act* which directs the release of certain information for the purpose of facilitating customer transfers or (in the case of the electricity industry) wholesale market settlement.

PART 3 EXPLICIT INFORMED CONSENT FOR CONTRACTS

4 WHEN EXPLICIT INFORMED CONSENT IS REQUIRED

4.1 Entering into a *contract*

The *explicit informed consent* of a *customer* is required by virtue of clause 22.1⁹ of the relevant *Retail Code*, in connection with a *contract* between the *customer* and a *retailer* commencing to be effective, if:

- the *contract* includes a term or condition which is inconsistent with a term or condition set out in the *Retail Codes* marked with an asterisk (*); or
- the *customer* is transferring to the *retailer*.¹⁰

⁹ For Gas *Retail Code* from 2 July 2002.

¹⁰ A *customer's* consent is required in entering into all other sorts of *contract*, such as *contracts* arising from the acceptance of *standing offers* which are wholly consistent with a *Retail Code*. Despite not regulating for this in this guideline, the *Commission* expects that *retailers* will ensure that the consent of any *customer* to enter into such a *contract* also is informed and that *retailers* will keep a record of such consent having been given.

4.2 Estimated bills and different billing cycles

The *explicit informed consent* of a *customer* is also required by virtue of:

- clause 5.1 of the *Retail Codes*, if a *retailer* wants to base the *customer's* bill other than on a reading of the *customer's* meter; and
- by virtue of clause 10.1 of the *Retail Codes*, if a *retailer* and the *customer* want to agree a billing cycle other than that specified in the relevant *Retail Code*.

4.3 Scope of this Part 3

The scope of this Part 3 is limited to defining what *explicit informed consent* is for the purposes of the provisions of the *Retail Codes* referred to in clauses 4.1 and 4.2 and the *Gas Retail Rules*. This Part 3 does not deal with the requirement for consent in connection with the use or disclosure by a *retailer* of *customer information*. That is dealt with in Part 2.

5 REQUIREMENTS FOR CONSENT TO BE EXPLICIT AND INFORMED

5.1 General Requirements

For consent to be *explicit informed consent* the consent must be:

- given by a *customer* to a *retailer* explicitly as contemplated by clause 5.2 (that is, “opt-in” consent). It is not sufficient that consent is given implicitly (that is, “opt-out” consent);
- informed; and
- given by a person competent to give it.

5.2 Explicit consent

5.2.1 A *customer's explicit informed consent* is consent given:

- in *writing* signed by the *customer*;
- by *electronic communication* signed by the *customer*¹¹; or
- verbally.

5.2.2 Despite clause 5.2.1, a *customer's explicit informed consent* in the circumstances contemplated by clause 4.2 must be given either in *writing* signed by the *customer* or by *electronic communication* signed by the *customer*. It is not sufficient that consent is given verbally.

¹¹ Under section 9 of the *Electronic Transactions (Victoria) Act 2000*, an *electronic communication* is likely to be taken to have been signed if a method is used to identify the *customer* and to indicate the *customer's* approval of the consent and, having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the consent was communicated.

5.3 Consent must be informed

In order for a person to be considered to have consented to something, that person must know what that consent applies to. The *Commission* will assume the requisite knowledge in relation to a consent if the circumstances are such to suggest that the consent was informed. In this regard, the chances of a *customer's* consent to something being considered to have been informed are increased the more clear it is that the *customer* would have been aware, when providing consent, what that consent applied to. For example, in most circumstances a *customer's* consent would be considered to have been informed if:

- (a) the relevant *retailer* has fully and adequately disclosed all matters relevant to the consent to the *customer* including each specific purpose or use of the consent;¹² and
- (b) those matters are disclosed clearly and in plain English

5.4 Competence and capacity

5.4.1 If it can be established that a person has given consent, the *Commission* would generally be prepared to assume that the person was competent to do so. General rules of relevance to competence, however, apply in these circumstances. In this regard:

- (a) in order for a *customer* to be competent to give consent, the *customer* must be capable of understanding issues, forming views based on reasoned judgement and communicating their decision; and
- (b) in order for a person to be competent to give consent on behalf of another, the person must have legal authority to do so.

5.4.2 A minor will generally be assumed not to be competent to provide consent to a contract unless the relevant retailer can establish that the preconditions to the validity of such a contract are satisfied.

Whether such preconditions are satisfied is, in essence, a legal question. The Commission will, however, be generally prepared to assume that they are satisfied in the case of retail to a site where no adult resides, but will otherwise assume they are not (in the absence of a court decision or special circumstances warranting a different conclusion).

6 RECORD KEEPING

6.1 *Explicit informed consent must be verifiable and auditable*

¹² In the context of a *contract* between a *retailer* and a *customer*, the *Retail Codes* supplement the *Fair Trading Act 1999* by requiring the *retailer* to give the *customer*, within a two *business days* timeframe, a document setting out among other things the *tariff* and all of the terms and conditions of the *contract*. This information is provided so the *customer* can consider whether to exercise any cooling-off related right the *customer* may have to cancel the *contract* and so ensures that, in a broader sense, the *customer's* consent to the *contract* is informed.

- 6.1.1 A **retailer** must keep a record of any **explicit informed consent** given by a **customer** and retain that record for at least as long as the **retailer** has any related **contract** with the **customer**.¹³
- 6.1.2 If the **explicit informed consent** is given verbally, the record must be kept in **writing** or in a recording made by a listening device.¹⁴ **Retailers** must develop written procedures on verbal consent records management, and make these procedures available to **customers** on request.
- 6.1.3 Further to the above, an electricity **retailer**¹⁵ must have regard to the consent audit provisions of the **Marketing Code of Conduct**.

6.2 Access

On request, a **retailer** must provide a **customer** with access to the record of any **explicit informed consent** given by the **customer** and then kept by the **retailer**.

<p>PART 4 GENERAL</p>

7 GLOSSARY

In this guideline:

- (a) terms which appear **like this** and which are not otherwise defined in this glossary have the same meaning as in the **Retail Codes**; and
- (b) **breach** in relation to a **NPP**, is an act or practice that would constitute a breach of the **NPP** under the **Privacy Act**;

corporate client means, in relation to a **retailer**, a person who is a present, past, or **prospective customer** of the **retailer** but who is not a natural person;

corporate client information means, in relation to a **retailer**, information or opinions about a **corporate client** of the **retailer**, being information or opinions which:

- would constitute personal information for the purpose of the **Privacy Act** were the term "individual" used in the **Privacy Act** to apply to any type of **corporate client**; and
- was obtained or arrived at in the ordinary course of the **retailer's** business

¹³ Under the *Electronic Transactions (Victoria) Act 2000*, a requirement to record information in writing can generally be met in electronic form.

¹⁴ The consent of each party to the recording of a private conversation may be required under the *Surveillance Devices Act 1999*.

¹⁵ It is expected that the Marketing Code of Conduct shall also apply to the gas industry. However, at present, gas licence amendments to this effect have not been finalised.

as a *retailer*;

Commission means the Essential Services Commission under the *Essential Services Commission Act 2001*;

Credit Management Guideline means the electricity or gas guideline of that name issued by the Commission;

customer means, in relation to a *retailer*, a person who buys or proposes to buy gas or electricity from the *retailer* (and who is not, itself, a *retailer*).

customer information means, in relation to a *retailer*, information or opinions which constitute personal information for the purposes of the *Privacy Act*, being information or opinions about a natural person who is a present, past or prospective *customer* of the *retailer*;

Electricity Act means the *Electricity Industry Act 2000*;

Electricity Retail Code means the Code of that name setting out terms and conditions relevant to contracts for the supply or sale of electricity first determined under the *Electricity Industry Act 2000* on 27 October 2000;

electronic communication has the same meaning as in the *Electronic Transactions (Victoria) Act 2000*;

explicit informed consent means consent given by a customer in circumstances where applicable requirements of clause 5 have been complied with;

Gas Act means the *Gas Industry Act 2001*;

Gas Retail Code means the code of that name setting out the terms and conditions for contracts for the supply or sale of gas to certain *customers*, first determined by the *Office* in May 2001, for effect on 1 September, 2001;

Gas Retail Rules means Retail Gas Market Rules within the meaning of the *Gas Act*;

Industry Act means the *Electricity Act* or the *Gas Act*;

Marketing Code of Conduct means the electricity Code¹⁶ of that name issued by the Commission;

NPPs means the National Privacy Principles, within the meaning of the *Privacy Act*;

Privacy Act means the Privacy Act 1988 (Commonwealth);

Private Sector Privacy Act means the *Privacy Amendment (Private Sector) Act 2000* (Commonwealth);

¹⁶

It is expected that the Marketing Code of Conduct shall also apply to the gas industry. However, at present, gas licence amendments to this effect have not been finalised.

Retail Code means the *Electricity Retail Code* or the *Gas Retail Code*;

retail licence means a licence granted under an *Industry Act* to sell electricity other than through the wholesale electricity market operated by National Electricity Market Management Company Limited (ACN 072 010 327) or to sell gas by retail;

retailer means a person who holds a *retail licence*; and

writing includes any mode of representing or reproducing words, figures, drawings or symbols in visible form other than *electronic communication*.

7.1 General

- (a) a reference to any legislation (including an *Industry Act*) or to any provision of any legislation includes any modification or re-enactment of, or any legislation or provision substituted for, and all regulations, proclamations, orders in council and by-laws issued under, the legislation or the provision;
- (b) words denoting a gender include any gender;
- (c) the term "including" means "including, without limitation";
- (d) headings are not intended to affect the interpretation of this guideline;
- (e) a reference to a person includes that person's successors and assigns;
- (f) a reference to a body (including the *Commission*) either which ceases to exist or whose powers or functions are transferred to another body is a reference to the body which replaces it or which substantially succeeds to its powers or functions;
- (g) a reference to this guideline, a *NPP*, a code or an instrument is a reference to this guideline, the *NPP*, the code or instrument as amended, varied or replaced from time to time.

ATTACHMENT: THE NATIONAL PRIVACY PRINCIPLES

1 Collection

- 1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.
- 1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.
- 1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
 - (a) the identity of the organisation and how to contact it; and
 - (b) the fact that he or she is able to gain access to the information; and
 - (c) the purposes for which the information is collected; and
 - (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
 - (e) any law that requires the particular information to be collected; and
 - (f) the main consequences (if any) for the individual if all or part of the information is not provided.
- 1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.
- 1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the *secondary purpose*) other than the primary purpose of collection unless:
 - (a) both of the following apply:
 - (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
 - (ii) the individual would reasonably expect the organization to use or disclose the information for the secondary purpose; or
 - (b) the individual has consented to the use or disclosure; or
 - (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
 - (i) it is impracticable for the organisation to seek the individual's consent before that particular use; and
 - (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
 - (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

- (iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and
- (v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or
- (d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:
 - (i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or
- (e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:
 - (i) a serious and imminent threat to an individual's life, health or safety; or
 - (ii) a serious threat to public health or public safety; or
- (f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (g) the use or disclosure is required or authorised by or under law; or
- (h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

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

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

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

- 2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.
- 2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.
- 2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
- (a) the individual:
 - (i) is physically or legally incapable of giving consent to the disclosure; or
 - (ii) physically cannot communicate consent to the disclosure; and
 - (b) a natural person (the *carer*) providing the health service for the organisation is satisfied that either:
 - (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
 - (ii) the disclosure is made for compassionate reasons; and
 - (c) the disclosure is not contrary to any wish:
 - (i) expressed by the individual before the individual became unable to give or communicate consent; and
 - (ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and
 - (d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).
- 2.5 For the purposes of subclause 2.4, a person is *responsible* for an individual if the person is:
- (a) a parent of the individual; or
 - (b) a child or sibling of the individual and at least 18 years old; or
 - (c) a spouse or de facto spouse of the individual; or
 - (d) a relative of the individual, at least 18 years old and a member of the individual's household; or
 - (e) a guardian of the individual; or
 - (f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or
 - (g) a person who has an intimate personal relationship with the individual; or
 - (h) a person nominated by the individual to be contacted in case of emergency.
- 2.6 In subclause 2.5: *child* of an individual includes an adopted child, a step-child and a foster-child, of the individual.

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

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

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

3 Data quality

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

4 Data security

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

5 Openness

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

6 Access and correction

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

-
- (i) providing access would be likely to prejudice an investigation of possible unlawful activity; or
 - (j) providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (iii) the protection of the public revenue; or
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
 by or on behalf of an enforcement body; or
 - (k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

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

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

- 6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.
- 6.4 If an organisation charges for providing access to personal information, those charges:
 - (a) must not be excessive; and
 - (b) must not apply to lodging a request for access.
- 6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.
- 6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.
- 6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

- 7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
- (a) an agency; or
 - (b) an agent of an agency acting in its capacity as agent; or
 - (c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.
- 7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

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

- 7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:
- (a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or
 - (b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or
 - (c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

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

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

8 Anonymity

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

9 Transborder data flows

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

- (a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or
- (b) the individual consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

- (e) all of the following apply:
 - (i) the transfer is for the benefit of the individual;
 - (ii) it is impracticable to obtain the consent of the individual to that transfer;
 - (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

- 10.1 An organisation must not collect sensitive information about an individual unless:
- (a) the individual has consented; or
 - (b) the collection is required by law; or
 - (c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
 - (i) is physically or legally incapable of giving consent to the collection; or
 - (ii) physically cannot communicate consent to the collection; or
 - (d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
 - (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
 - (ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
 - (e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.
- 10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:
- (a) the information is necessary to provide a health service to the individual; and
 - (b) the information is collected:
 - (i) as required 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.
- 10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:
- (a) the collection is necessary for any of the following purposes:
 - (i) research relevant to public health or public safety;
 - (ii) the compilation or analysis of statistics relevant to public health or public safety;
 - (iii) the management, funding or monitoring of a health service; and

- (b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
- (c) it is impracticable for the organisation to seek the individual's consent to the collection; and
- (d) the information is collected:
 - (i) as required by law (other than this Act); or
 - (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
 - (iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

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

10.5 In this clause:

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