ENERGY AND WATER OMBUDSMAN
Victoria Listen Assist Resolve

Privacy Policy

ENERGY AND WATER OMBUDSMAN (VICTORIA)

January 2019

Table of Contents

Overview and objective

EWOV is committed to protecting the privacy of customers who contact EWOV requesting information or wishing to make a complaint. EWOV complies with the requirements of Australian privacy laws, including obligations under the Commonwealth *Privacy Act 1988* (Privacy Act) and the *Australian Privacy Principles* (APPs).[1] The APPs form part of EWOV's Privacy Policy.[2] Full text of the APPs is available from the Office of the Australian Information Commissioner ('OAIC').

EWOV receives, investigates and facilitates the resolution of customer complaints about electricity, gas and water providers operating in Victoria. EWOV's services are free to customers.

As an industry-based external dispute resolution scheme, EWOV collects, handles and manages personal information[3] in order to assist with the receipt, investigation and resolution of customer complaints about electricity, gas and water providers.

All collection, use and disclosure of personal information by EWOV will be done for the purposes of complaint investigation and resolution or for associated purposes, such as reporting to government bodies and regulators and continuing operational and service improvement.

This policy outlines how EWOV collects, uses, discloses and stores personal information to ensure that the privacy of customers dealing with EWOV is protected.

Collection, use, disclosure and storage of personal information

Customers covered by EWOV's Privacy Policy

The Privacy Act and APPs provide protection for individuals regarding how their personal information is collected, handled and stored.

Although companies and businesses are not accorded the same protection as individuals under Australia's privacy laws, EWOV considers that individuals, companies and businesses are all "customers". EWOV will treat personal information relating to any customer as information requiring confidentiality and in accordance with this policy.[4]

[1] This Policy has been drafted in order to comply with obligations under the APPs which come into force on 12 March 2014. Until that time, EWOV complies with obligations under the National Privacy Principles (NPPs). This policy is intended to meet EWOV's obligations under both the NPPs and the APPs.

[2] See Appendix 1 for a plain English summary of the APPs.

[3] ***Personal information*** is information which identifies, or could reasonably identify an individual. Obvious examples include a person's name or address, but personal information could include medical records, bank account details, photos or information about a person's opinions or where they work. Information does not have to include someone's name to be personal information. ***Personal information*** is defined in the *Privacy Act* as meaning "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."

[4] This is consistent with obligations in EWOV's Charter (clause 4.1) which specifically require the Ombudsman to act in accordance with accepted privacy laws with respect to all information concerning or relating to a complaint.

Anonymity and Pseudonymity[5]

Customers have the option of staying anonymous or using a pseudonym when contacting EWOV.

EWOV asks callers to identify themselves and to provide a postcode for reporting purposes and to enable assessment of the geographical spread of callers. However, customers with a general enquiry not related to a specific complaint will not be required to identify themselves.

Due to the nature of dispute resolution, it is not practicable for EWOV to investigate complaints where customers remain anonymous or use a pseudonym. Customers wishing to make a complaint will be required to identify themselves.

Collection[6]

EWOV collects personal information for the purpose of dispute resolution. Given EWOV's purpose, function and activities, it is assumed that before most customers contact EWOV, they will be aware that EWOV will use any personal information provided to investigate and resolve their complaint. It is also assumed most customers would be aware the investigation process will require collection and disclosure of personal information to relevant providers and possibly independent EWOV experts/advisors.

Collection of personal information by EWOV will be done by fair and lawful means and will not be done in an unreasonably intrusive way. EWOV will not accept personal information obtained unlawfully.

EWOV collects information in the following ways:

1. Orally from a customer, a customer's representative or a provider by telephone or in person
2. In writing from a customer, a customer's representative or a provider whether by electronic or other means
3. From third parties where relevant and appropriate, provided the customer has previously been made aware of, and has consented to, this course of action

Where EWOV collects personal information, EWOV provides the customer with information required by the APPs[7] using a combination of the following:

- a privacy statement on EWOV's website

[5] APP 2

[6] APP 3, APP 4 and APP 5

[7] Such as:

- EWOV's identity and how to contact us
- If EWOV collected the information from someone other than the customer, the fact of, and circumstances around the collection
- Whether the collection is required or authorised by law and details or any law or order requiring or authorising the collection
- The purposes for which EWOV has collected the information
- The main consequences for a customer if all or some of the information is not collected
- The organisations or types of organisations to which EWOV normally discloses this type of information
- That EWOV's Privacy Policy has information about how the customer can gain access to, and seek correction of, the information
- That EWOV's Privacy Policy has information about how the customer can complain about a privacy breach and how EWOV will deal with such breaches
- Whether EWOV is likely to disclose the information to overseas recipients

- a privacy statement in correspondence to customers
- advising customers of the existence of its Privacy Policy and how to access the policy
- providing the information on request

Where reasonable and practicable, EWOV collects personal information about a customer directly from that customer.

Third party and unsolicited information[8]

From time to time, EWOV receives information about a third party who has no active interest or involvement in a complaint. Sometimes EWOV receives third party personal and unsolicited information from both providers and customers.[9]

It is accepted practice for alternative dispute resolution schemes such as EWOV to collect and use all available information, including third party personal information, in order to carry out the primary purpose of complaint resolution.

If EWOV has collected personal information about a third party, EWOV will not contact the third party directly to advise of the collection of information because to do so would breach the confidentiality of the customer, and may pose a threat to the life, health and safety of the customer.

For these reasons, EWOV has determined that it is not reasonable or practicable for EWOV to inform the third party of the matters required by the APPs (see above at footnote 7).

In the case of joint account holders, where one account holder makes a complaint and the other does not, EWOV will ask the complainant to advise the other account holder that the complaint has been made.

Information collected online by EWOV

It is EWOV's usual practice to collect information about all visitors to our online resources. That information is very limited and only used to identify generic behavioural patterns.

Sometimes EWOV uses third party platforms to deliver information. These sites are hosted and managed by organisations other than EWOV. A customer should read the privacy policy of any third party before deciding if they want to contribute to any such site.

There are several methods and packages that EWOV uses to collect visitor behaviours on each of our online platforms. EWOV uses Google Analytics on our website. Information and data collected through Google Analytics is stored by Google on servers in the United States of America, Belgium and Finland. A customer can opt out of

- The countries in which overseas recipients of information are likely to be located, if disclosure to overseas recipients is probable

[8] APP 4

[9] Examples include:
- Personal information contained in contact notes given by a provider during the course of an investigation
- Personal information from a customer about provider staff member/s (which may have nothing to do with the current complaint)
- Personal information from a customer about a neighbour's situation which the customer believes is similar to their own, such as a neighbour's claim being paid following an outage or voltage variation, but their own claim being denied

the collection of information via Google Analytics by downloading the Google Analytics Opt-out browser ad on (https://tools.google.com/dlpage/gaoptout?hl=en-GB).

When a customer visits any of EWOV's online resources, our metric tools may collect the following information about the visit for statistical purposes:

- Server address
- Top level domain name (for example .com, .gov, .au, .uk etc.)
- The date and time of your visit to the site
- The pages a customer accessed and the documents downloaded during the visit
- The previous site a customer visited
- Whether the customer has visited EWOV's site before
- The type of browser used.

EWOV records this data to maintain our server and improve our services. EWOV does not use this information to personally identify anyone.

Most of EWOV's online platforms use sessions and cookies. The core functionality on these platforms will be largely unaffected if a customer disables cookies in their browser but they may be unable to access some advanced functions.

Use and disclosure[10]

EWOV uses and discloses personal information collected for the primary purpose of dispute resolution.

EWOV will not disclose personal information to another party if a customer explicitly denies consent for the disclosure. However, where a customer denies consent to the disclosure of personal information, EWOV may be limited in the further assistance which can be offered, and may be obliged to close the customer's complaint.

EWOV will only use or disclose personal information for a secondary purpose if:

1. The customer has consented to the use or disclosure; or
2. The customer would reasonably expect EWOV to use or disclose the information and the secondary purpose is related or directly related[11] to the primary purpose; or
3. EWOV is legally required or authorised to use or disclose the information; or
4. EWOV is entitled to use or disclose the information because of an exception in the APPs.

In order to investigate or resolve a complaint, EWOV may disclose personal information to providers, third party experts/advisors or other agencies, such as government regulators. Third party independent experts/advisors engaged by EWOV are required to sign a confidentiality agreement prior to customer information being disclosed.

[10] APP 6

[11] The secondary purpose needs to be directly related if the information is sensitive information

When reporting to relevant bodies, such as government agencies or regulators, EWOV provides de-identified information. If EWOV is asked for personal information relating to any reported complaints, EWOV will seek consent from a customer prior to any disclosure, and will not disclose information if consent is not provided.

To ensure EWOV provides an effective and efficient level of service, EWOV may disclose customer information to market research companies for the purpose of customer satisfaction surveys. The market research company is required to sign a confidentiality agreement and provide all information back to EWOV. If a customer decides to "opt out" of the survey process, EWOV's records will be notated accordingly.

EWOV does not engage in any direct marketing activities, and will not provide a customer's personal information to another body for the purposes of direct marketing.

Where a customer has copied correspondence to a third party, this does not constitute authority enabling EWOV to discuss the complaint with that third party or for them to receive information about the progress of the complaint; EWOV staff only disclose information about a complaint to the customer or their authorised representative. EWOV's fact sheet titled *Acting on behalf of someone with an EWOV complaint* provides detail about the way EWOV seeks authority from a customer, as well as how and when an Authority to Act form will be obtained.

Sensitive information[12]

Sensitive information includes information about an individual's:

a. Racial or ethnic origin
b. Political opinions or associations
c. Religious or philosophical beliefs or affiliations
d. Memberships held with professional or trade associations or unions
e. Sexual orientation or practices
f. Criminal record
g. Health
h. Biometric information13

EWOV will limit the collection, use, and disclosure of sensitive information to instances where the sensitive information is directly relevant and reasonably necessary for the investigation and resolution of a complaint made to EWOV.

[12] See the Privacy Act (Part II, s6) for full definition of ***sensitive information***

[13] Biometric information or identifiers are distinctive, measurable characteristics or traits which can be used for identification of an individual. The most common types of biometric information or identifiers are things such as fingerprints, face recognition, DNA, palm prints, hand geometry, iris recognition, retina, odour/scent, typing rhythm, gait and voice.

Examples where the collection and handling of sensitive information may be directly relevant and reasonably necessary to EWOV's dispute resolution function are:

1. Details of health problems or illness (chronic, intermittent or temporary), imprisonment or unemployment (recent or long-term) which may have impacted the customer's ability to service their account. The purpose of providing the information may be to seek leniency, reconsideration or assistance from the provider, or to consider the legality of the provider's actions having regarding to the circumstances (eg. compliance with hardship requirements prior to disconnection).
2. Details of mental or physical health or other personal circumstances of the customer or others (such as dependents, family members) which may be directly relevant to the question of whether the provider has acted appropriately.

Where a customer volunteers or provides sensitive information to EWOV, consent to the collection, storage and use of the sensitive information will be assumed.

Data quality, access and correction[14]

EWOV will take reasonable steps to make sure that the personal information collected, used or disclosed is accurate, complete and up-to-date.

EWOV will make the necessary changes to personal information details held where a customer or provider notifies EWOV of errors or changes required. EWOV will make the changes as soon as practicable.

If EWOV does not agree to make requested changes to personal information, the customer may make a statement about the requested changes and EWOV will attach this statement to the customer's record.

EWOV will provide access to personal information to the customer concerned upon request and within a reasonable period unless one or more of the exceptions in the APPs applies.[15]

EWOV will provide written reasons for a denial of access or a refusal to correct personal information, including mechanisms available to complain about the denial of access or refusal to correct. EWOV will provide access to personal information free of charge.

A customer wanting to access their personal information held by EWOV should make a request to the Conciliator investigating their complaint or to the Privacy Officer:

The Privacy Officer
EWOV
GPO Box 469
Melbourne 3001
Email: ewovinfo@ewov.com.au

[14] APP 10, APP 12 and APP 13

[15] Exceptions include:
- Providing access would pose a serious and imminent threat to someone's life or health
- Providing access would have an unreasonable impact on someone else's privacy
- The request for access is frivolous or vexatious
- Providing access would be unlawful or prejudicial as described in clauses 12.3(d) to (j) of the APPs.

Data security[16]

EWOV will take reasonable steps to protect the personal information held from misuse, loss or unauthorised access, modification or disclosure.

These steps include electronic security for EWOV's premises and information systems, password protection for electronic files and securing paper files in locked cabinets.

EWOV will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for the purposes of dispute resolution or associated purposes.

EWOV needs to reference historical complaint data for a number of reasons, including:

- Analysis and reporting to government bodies and regulators
- Retaining a full picture of a customer's complaint history - this can be relevant when a customer re-contacts EWOV with continuing issues or re-emergence of a dispute, even years after the initial complaint is resolved
- To assist in assessing what is fair and reasonable for other similar complaints, as EWOV has regard to previous complaint circumstances and outcomes in such assessments
- Continuing operational and service improvement, including staff training

As the personal information collected is intrinsically embedded into EWOV's electronic records, it is not practicable to de-identify or remove personal information without losing the integrity of the data. For these reasons, EWOV retains complete electronic records indefinitely.

EWOV's databases keep audit trails when the records are accessed, amended or deleted.

EWOV digitally records telephone calls for quality and training purposes. In some instances, a call recording may be attached to an electronic record.

Remote access – electronic and paper files

Some EWOV staff members have authority to remotely access EWOV's information technology (IT) systems. EWOV's Privacy policy is still applicable when accessing EWOV's IT systems remotely.

EWOV staff are expected to ensure their computers are password protected so that unauthorised individuals cannot access EWOV documents or electronic files. EWOV staff should not leave a computer logged in if it is unattended, and should ensure that no residual copies are retained on a computer after they have accessed an electronic file.

EWOV staff should not leave printed/hard copy customer files, provider records or printed documents at any remote location, including a home desk. If bringing confidential information to and from work, EWOV staff must ensure any documentation or records are secure with no loose papers which could easily be lost. Permission must

[16] APP 11

be obtained from a Team Manager or the General Manager Operations if EWOV Conciliation team staff wish to remove confidential documents from the office.

Any confidential information printed remotely needs to be disposed of in the designated recycling bin for confidential waste at EWOV.

Identifiers[17]

EWOV does not, and will not, use any government assigned identifier, such as a Tax File or Medicare number, to identify customers.

EWOV uses case references which take the form YYYY/# in chronological order of registration. Individuals are not assigned any identifying number or code by EWOV. Where a customer makes more than one complaint to EWOV, each complaint will have a separate case reference number.

Cross-border disclosure[18]

As EWOV's jurisdiction does not extend to overseas electricity, gas or water businesses, it is unlikely EWOV will need to transfer or disclose personal information about a customer to someone overseas, other than the customer (or their authorised representative).

EWOV discloses customer email addresses to Survey Monkey for the purpose of customer satisfaction surveys. Information collected by Survey Monkey is stored on servers in the United States of America. A customer can opt out of having their email address used for the purpose of surveying by advising their case handler.

EWOV's intranet test server is hosted by Amazon in the United States of America. The server is used to test general functionality and intranet application upgrades.

EWOV's IT networks and systems mainly use servers and support within Australia. However, should EWOV need to transfer or disclose personal information overseas, EWOV will seek consent for the transfer or disclosure, or ensure it otherwise complies with obligations under the APPs.

Contacting EWOV

If customers have a complaint about the way in which EWOV has handled their personal information, they should contact:

The Privacy Officer
EWOV
GPO Box 469
Melbourne 3001
Email: ewovinfo@ewov.com.au

[17] APP 9

[18] APP 8

EWOV takes complaints about potential privacy breaches seriously. EWOV will investigate the circumstances of a privacy complaint and will undertake remedial action required, including any necessary staff training.

If customers are not satisfied with EWOV's response, customers may wish to contact the Office of the Australian Information Commissioner:

GPO Box 5218 Sydney NSW 2001
GPO Box 2999 Canberra ACT 2601

Email - **enquiries@oaic.gov.au**

Phone: **1300 363 992**

Document history

Action	Updated By	Date
Redrafted	JVE	March 2014
Amended content 'Cross-border disclosure'	EN	July 2015
Amended content 'Cross-border disclosure'	EN	May 2016
Amended Charter reference	HMN	August 2018
Amended content: Updated with new processes for handling third party and sensitive information	HMN	January 2019
Updated format, removed full text of APPs	GP	January 2019

Appendix

Plain English Summary of the Australian Privacy Principles[19]

There are 13 APPs that regulate how government agencies and private sector organisations manage personal information. They cover the collection, use and disclosure, and secure management of personal information. They also allow individuals to access that information and have it corrected if it is wrong.

APP 1: management of personal information
Aims to ensure organisations manage personal information in an open and transparent way. Organisations need to take steps to ensure compliance with the APPs and must have a clearly expressed and up-to-date privacy policy which is publicly available. APP 1 also outlines information which must be included in a privacy policy.

APP 2: anonymity and pseudonymity
Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves or by using a pseudonym.

APP 3: collection of solicited personal information
Describes what an organisation should do when collecting personal information, including sensitive information (eg. health, racial or ethnic background, or criminal record) or information from third parties. Higher standards apply to the handling of sensitive information.

APP 4: dealing with unsolicited personal information
Describes what an organisation should do when it obtains information which it did not seek or request. Organisations are required to destroy or de-identify personal information which cannot be collected under APP 3.

APP 5: notification of collection
Describes what an organisation needs to tell individuals about the collection of information.

APP 6: use and disclosure
Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information.

APP 7: direct marketing
Outlines the rules about direct marketing.

APP 8: cross-border disclosure
Outlines how organisations should protect personal information that they transfer outside Australia.

APP 9: identifiers
Generally prevents an organisation from adopting an Australian Government identifier for an individual (eg. Medicare numbers) as its own.

[19] Summary of the Australian Privacy Principles from www.oaic.gov.au

APPs 10 and 11: information quality and security

An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

APP 12 and 13: access and correction

Give individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.