Privacy Policy

July 2025

Energy & Water Ombudsman Queensland

Contents

Scope

About this policy

This privacy policy covers the Energy and Water Ombudsman Queensland.

The *Information Privacy Act 2009* (**IP Act**) sets out how the Energy and Water Ombudsman Queensland (**EWOQ** or **we** or **us**) must manage personal information. It also sets out how people can access their personal information (if it is information we hold) and how they can request changes to it.

Under the IP Act, we must keep personal information responsibly and collect it transparently. We must follow the Queensland Privacy Principles (**QPPs**) within the IP Act that set out how personal information must be collected, stored, secured, accessed, amended, used and disclosed. The IP Act also:

a. sets out the requirements for us to transfer personal information outside of Australia;

b. lists the rules regarding contracted service providers;

c. creates a right for individuals to access and amend their personal information; and

d. provides a complaint mechanism for any act or practice that is a breach of the QPPs.

As well as the obligations we must comply with under the IP Act, section 79 of the *Energy and Water Ombudsman Act 2006* also prohibits disclosure of information obtained while performing a function under the Act unless the disclosure is for a specified purpose. In practice, this means that we will disclose personal information provided to us by customers to the scheme participant (the customer's energy or water supplier/distributor) complained about so that we can obtain their response to the complaint or seek clarification of issues or further information.

Recent reforms commencing 1 July 2025 include the introduction of a Mandatory Data Breach Notification Scheme which EWOQ is required to comply with.

The aim of this policy is to assist members of the public, EWOQ staff, contractors and consultants to understand how personal information is managed by EWOQ, and to set out the ways in which we use and store personal information.

Who this policy applies to

This policy lists our obligations in relation to the collection, management, use and disclosure of personal information held by us.

The people who must comply with the obligations set out in this plan are:

- all EWOQ employees;
- work experience staff and trainees;
- any person or entity engaged by us to provide a service, information or advice; and
- selection panel members involved in the recruitment of our staff.

Overall responsibility for the proper use of personal information rests with our Ombudsman. However, all team members are responsible for ensuring that they comply with the IP Act and this policy in relation to the collection, management, use and disclosure of personal information that we hold. Employees are given access only to information which is relevant to their duties.

The day-to-day organising of information privacy has been delegated to the Information Privacy Officer who is the first point of contact for members of the public and employees when they have a

question or concern about privacy and personal information. The Information Privacy Officer is responsible for:

- monitoring compliance with the IP Act, reporting on IP Act matters and providing general information on privacy-related issues;
- dealing with requests to amend records containing personal information;
- dealing with suspected breaches of privacy, including suspected data breaches and privacy complaints; and
- conducting privacy audits.

The Information Privacy Officer can be contacted at **rti&ip@ewoq.com.au** or by phone on **1800 662 837**.

Personal information

What is personal information?

'Personal information' is defined in the IP Act as:

> information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion—
>
> (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. For clarity, personal information is not necessarily sensitive or confidential, and it doesn't need to directly identify the individual. If their identity could be discovered by taking a series of steps (for example, by combining several pieces of information to work out which individual is being referred to) then this may be personal information.

As personal information relates to information about individuals, corporations do not have privacy rights under the IP Act.

What is not personal information?

The IP Act sets out some kinds of documents which, even if they include what would otherwise be considered personal information, do not have the same protections. These include documents concerning:

- covert operations of law enforcement agencies;
- witness protection;
- certain complaints and investigations of misconduct under the *Police Service Administration Act 1990* and the *Crime and Corruption Act 2001*;
- public interest disclosures made under the *Public Interest Disclosure Act 2010*;
- Cabinet and Executive Council; and
- commissions of inquiry.

The QPPs also do not apply to a document that is a generally available publication (that is, a document which is normally available to the public). Information about a deceased person is also not considered personal information for the purposes of the IP Act.

What information we collect

We collect certain kinds of personal information regularly as part of the work we do in resolving disputes and running our office. We usually collect information from our customers (people who contact us with a complaint to resolve) when they first get in touch with us or throughout the course of resolving a complaint (and sometimes at other times when we are contacted by customers generally). We also collect relevant personal information of our team members and potential recruits.

Information we collect from our customers

We may collect personal information when customers contact us, use our service, complete our forms, visit our website or deal with us in some other way. We collect this information directly from the customer where appropriate or from an authorised person or representative acting on behalf of a customer.

We collect personal information from our customers so that we can properly provide our services.

The types of information we collect will vary depending on the activity, function or service we are engaging in and may include (but may go beyond if needed):

- their name[1]
- their contact details (e.g. current and previous addresses, telephone numbers, email address)
- how many people live at the home the complaint relates to
- account information (current and past) relevant to the dispute
- information the energy or water supplier or distributor gives to us about the customer
- other information provided to us by the customer, supplier or distributor (which might include photos of the property or meter and the like)
- information from collection agencies
- other demographic information (which is provided at the customer's choice and not a prerequisite to service)
- information about any special needs of the customer (for example, if they need an interpreter)
- when a customer visits our website, messages us on social media or uses our live chat – for example location information, IP address, device used, publicly available profile information and network information
- we may monitor or record calls for case management, training and coaching purposes. Customers can tell the operator if they don't want us to do this.

Consent

In most cases, unless otherwise notified, it is assumed that most customers who contact us for our dispute resolution service will be aware that we will use and disclose any personal information provided as needed to investigate and resolve the complaint.

Where we are provided with sensitive information, consent to the collection, storage and use will be assumed.

[1] While a customer can choose to stay anonymous, it is more difficult for us to investigate an anonymous complaint (depending on the details provided) and we will not be able to advise them of the outcome.

We may also obtain express consent to collect, use or disclose information for other types of activities and functions. For example, we ask for consent to be involved in customer experience surveys.

EWOQ has established processes that require customers acknowledge the sharing of information or advise they wish to opt out.

Customers can withdraw their consent for us to use, disclose and store any personal information by contacting us. However, in doing so this may limit our ability to provide our service or perform our function as a dispute resolution service. For example, we may be unable to:

- proceed or constructively engage in the investigation or resolution of a complaint
- refer a complaint to another dispute resolution service under our Memorandum of Understanding agreements.

Anonymity and pseudonymity

Personal information is required to verify customer details, to progress a complaint and provide the outcome of a complaint.

Where possible, we will provide for customers to interact with us anonymously or using a pseudonym. For example, if a customer calls us with a general question or submits an anonymous complaint through our website we will not ask for their name unless we need it to handle their question.

Information we collect through our websites and third parties

Our public website and scheme participant portal are hosted in Australia. We collect information about visitors to our website and scheme participant portal to identify generic behavioural patterns and improve our services. We do not use this information to personally identify anyone.

Cookies and other tracking technology

A cookie is a small text file that is placed on the computer of a visitor to our website, that enables us to: (a) recognise the visitors computer; (b) store their preferences and settings; (c) understand the web pages of the services they have visited and the referral sites that have led them to our services; (d) enhance their user experience by delivering content specific to their inferred interests; (e) perform searches and analytics; and (f) assist with security administrative functions.

Most browsers allow users to choose whether to accept cookies or not. If a user does not wish to have cookies placed on their computer, they must set their browser preferences to reject all cookies before accessing our websites. Cookies can be deleted by the user in their browser settings.

Tracking pixels (sometimes referred to as web beacons or clear GIFs) are tiny electronic tags with a unique identifier embedded in websites, online ads and/or email. We may use this technology to provide usage information like ad impressions or clicks on our social media advertising. Information collected by tracking pixels on our social media is governed by the privacy policy of the platform being used and must be accepted by customers to use those services.

If a customer signs up to receive email from us, we may use other analytic tools (such as Vision6) to capture data about whether the email is opened, links are clicked or otherwise interacted with the email. This allows us to measure the effectiveness of our communications and marketing campaigns.

Web analytics

We use third party analytic services (such as Microsoft, Google Analytics and Acquia Optimize) to collect non-personal data about interactions on our website. The sole purpose for collecting this data using these services is to improve the experience for people using our website.

These services use cookies to gather information such as:

- the number of visitors to EWOQ's website
- how visitors arrive at EWOQ's website, for example, did they type the address in directly, follow a link from another webpage, or arrive via a search engine?
- the number of times each page is viewed and for how long
- time and date of visit
- geographical location of the visitor
- information about what browser was used to view the website and the operating system of the computer
- information about whether the browser supports Java and Flash
- the speed of the user's internet connection.

A visitor can opt out of the collection of information via Google Analytics by downloading the Google Analytics Opt-out browser add-on from: **tools.google.com/dlpage/gaoptout?hl=en-GB**.

Google reCAPTCHA

We use Google reCAPTCHA to ensure the security of our website and the information provided through it. reCAPTCHA collects information like IP address, mouse movements, and dwell time to distinguish between human users and bots and prevent fraudulent or malicious activity on our website.

The information collected using this service will be collected directly by Google, who uses the information to evaluate use of their services. This information is stored outside of Australia. No personally identifying information is recorded or provided.

To use our online forms, customers must accept the Google Privacy Policy. If they do not wish to do so, they can call us or use our live chat.

Embedded videos

We use YouTube to embed videos and recordings of webinars and events on our website, and use of these services falls under the YouTube Privacy Policy.

Third party privacy policies and data storage

Information collected by third parties is generally stored in Australia but can include locations in the United States, Belgium, Ireland and Finland.

The privacy policies for third party technologies used by EWOQ are available through:

- Google: **policies.google.com/privacy**
- Microsoft: **privacy.microsoft.com/en-US/privacystatement**
- Acquia: **acquia.com/about-us/legal/privacy-policy**

- Vision6: **vision6.com.au/privacy-policy/**
- YouTube: **youtube.com/intl/ALL_au/howyoutubeworks/our-commitments/protecting-user-data/**

Information we collect from our team members and recruits

Employee information

We collect and store certain employee-related information because we are required to by law. Employee records include details about personnel, payroll, recruitment, performance and other records. The information collected may include names, dates of birth, occupation, employee identification number, general medical information, qualifications, next of kin, relationship details, details of pay and allowances, travel records, personal financial information, leave details, timesheet information and overtime records, work reports, employment history, staff awards, disciplinary investigations and actions, performance assessments and criminal convictions.

Recruitment information

We keep personal information provided by potential recruits, including applications to work with us, records relating to referee checks, interview notes and selection panel assessments.

As part of our screening process, criminal history checks may be undertaken in accordance with a consent form from applicants.

Copies of identification documents may be obtained as part of the hiring process to verify identity and other information.

Authorised people or representatives

Customers may wish someone to contact us on their behalf or have us talk to a representative about their dispute, e.g. a paid representative, a financial counsellor, or a relative or friend. Information about how to complete a form to appoint a representative can be found on our website: www.ewoq.com.au.

Where a representative is appointed by a customer, we use the form to show that the customer agrees for us to ask their representative for information, to give information to that person and to speak to that person as if we were speaking to the customer. We treat information provided by or to an authorised representative in the same way we would treat with the information if it was the customer we were dealing with.

Use and disclosure of personal information

Information used by our team members

On a day-to-day basis any of our team members with responsibility for receiving and responding to enquiries (including responding to messages on our live chat or social media), conducting investigations or undertaking administrative activities (and any team member responsible for supervising activities) may have access to personal information.

Similarly, other team members who work on planning, managing systemic issues, creating policy or reporting may have access to personal information for the purposes of collating statistics, reporting (including case studies with identifying information removed, presentations, training and quality

checking), or developing or researching policies and procedures. The information used may include demographic information to better target our community engagement work, to report to other regulators and Government bodies, and otherwise to assist in developing our processes and services. Any of the work produced by these team members will only be published if the information is de-personalised.

Other team members responsible for the managing of information technology systems may have access to personal information for the purposes of maintaining and creating the platforms on which the data is stored.

Customers can tell us if they do not want us to use their personal information in these ways, or if they want more information on how we manage their personal information.

Information provided to other entities

We will also disclose personal information given to us by customers to the customer's energy or water supplier/distributor (the entity complained about) so that they can respond to the complaint or seek clarification of an issue or further information. This is required by the EWO Act. We may give access to this information through an online portal or via email or post.

A customer's personal information may also be provided to government entities with a legitimate interest in the information, provided EWOQ has the customer's consent or is required by law to do so, for example, by force of a subpoena.

If a complaint is not within EWOQ's jurisdiction we may, with the customer's consent, refer the complaint to government entities or other ombudsman schemes which have a legitimate interest in the information, for example:

- Queensland Office of Fair Trading
- Queensland Competition Authority
- Queensland Treasury (formerly Department of Energy and Climate)
- Department of Local Government, Water and Volunteers (formerly Regional Development, Manufacturing and Water)
- Australian Competition and Consumer Commission
- Australian Energy Regulator
- Queensland Ombudsman
- Australian Energy Market Commission
- Office of the Australian Information Commissioner[2]
- Office of the Information Commissioner.

[2] The EWOQ is a recognised external dispute resolution scheme (EDR) under section 35 of the *Privacy Act 1988 (Cth)*. Subject to the *Energy and Water Ombudsman Act 2006*, EWOQ will receive, investigate, facilitate the resolution of, make decisions and recommendations for, and report on, complaints within its scope about acts or practices of EWOQ scheme participants that may be an interference with the privacy of an individual under subsections 13(1) and/or 13(2) of the *Privacy Act 1988 (Cth).* EDR privacy complaints may be referred to the Office of the Australian Information Commissioner.

Customer feedback and surveys

A customer's personal information may also be used for undertaking internal or external surveys. Customers are given an opportunity in speaking with our team members to provide their explicit informed consent to be involved in the surveys or advise EWOQ that they do not wish to be surveyed.

Information which identifies customers who have consented to the survey (name and contact details only) may be provided to an external company solely for the purpose of that company conducting surveys on behalf of EWOQ.

Where stated on a survey, a customer's responses may be provided to members of our scheme (i.e. retailers and network service providers) for use in quality control and in improving services. This includes entities which do not have a direct relationship with the customer (e.g. retailers other than their own). We will only provide the substantive responses and not the names or contact details of the customer, but if the customer's responses have identified themselves then this information will not be removed before the information is given to the members of our scheme.

We use the information our customers provide in surveys to improve our processes and review our performance.

Our team members and recruits

On a day-to-day basis some of our team members (those who have appropriate authorisation and operational need) have access to personal information of other team members.

Employee information

Employee records include details about personnel, payroll, recruitment, performance and other records. The information is used for our internal human resource management, including assessing whether employees are complying with policies and procedures. This information may be accessible by certain team members, including the employee's manager and line managers and others as required and appropriate. This information is stored and kept confidential otherwise.

Certain employee information relating to payroll, leave, employee requests and contact information is stored in online portals operated by third party providers. These third-party providers are subject to confidentiality obligations and the IP Act under the terms of their engagement.

Recruitment information

The information we collect through recruitment activities is used so that we can select employees fairly and is provided to members (and relevant administrative assistants) of selection panels (including possible third-party panel members) for use in deciding the successful candidate.

Criminal history checks may be undertaken in accordance with a consent form from applicants. This information is used in hiring decisions and then deleted. A record is retained that a search was undertaken without the search results.

Copies of identification documents may be obtained as part of the hiring process to verify identity and other information. This information is deleted once a hiring decision is made.

Recruitment information may be processed and handled through third party platforms, such as other government services and Springboard (as part of SmartJobs). Our human resources contractors may have access to information provided as part of recruitment processes for use in assisting us with evaluating applicants.

Limited and specific personal information is disclosed to third parties as appropriate, including superannuation companies as nominated by the team member, the Australian Taxation Office,

organisations in receipt of payroll deductions and external medical/emergency personnel. Otherwise, information is only disclosed to third parties with the permission of the team member or as required by law (for example, to the Crime and Corruption Commission in connection with allegations of official misconduct).

Other information

We also store other kinds of information (some of which may be personal information) to assist us in running our workplace. This includes content like financial management information, complaints, mailing lists, details of stakeholder groups, communications and publications, audit outcomes, security and general management issues. We collect and store this kind of information in accordance with the IP Act.

Our contractors

We may enter contracts with other entities and people for work associated with the performance of our duties. Some of these contracts require the disclosure of personal information to third parties, or the collection of personal information by third parties on our behalf (including in the ways listed above).

We will take all reasonable steps to ensure that the entity or person we have an agreement with complies with the relevant obligations in the IP Act and their contract with us, and that any entity or person that has made an agreement with us after 1 July 2009 complies with these principles as if it were us.

We will also take steps to ensure that third party contracts or arrangements contain appropriate privacy clauses, or show the steps taken to require the contractor to comply with the IP Act and in particular compliance with the Mandatory Data Breach Notification Scheme (MDBN Scheme).

How we manage and store personal information

We store records (including personal information) on paper and electronically. We will deal with personal information provided to us (whether in person, in paper, over the phone or online) in accordance with legislative obligations and the IP Act. Electronic information is stored securely and protected by two-factor authentication. Hard copy information is stored securely in accordance with its sensitivity, including in locked cabinets and filing systems.

Our information management network regularly holds, stores and allows us to access our complaints management database. Our IT officers, consultants and the IT companies we contract with may have access to personal information (concerning internet and email usage and security) in accordance with the terms of their service agreements with us, which are subject to confidentiality and the IP Act.

Transferring information overseas

Under the IP Act, we can only transfer personal information outside Australia if:

- the person whose information it is agrees to the transfer; or
- the transfer is allowed because of another law; or
- there are reasonable grounds to believe that the transfer must be made to prevent or lessen a serious threat to the life, health, safety or welfare of an individual, or public health, safety and welfare; or
- two or more of the following apply:

- the person receiving the personal information outside of Australia is also bound to comply with privacy obligations that are substantially the same as the QPPs;
- the transfer is necessary to the work that we do for the person whose information it is;
- the transfer is for the benefit of the person whose information it is and it is not possible to seek their consent, but if sought it would likely be given; or
- reasonable steps have been taken to ensure the information is protected.

How to apply to us to see or change your personal information records

Except where we are not allowed because of another law, we are required (under QPP 12 and QPP 13) to allow a person to apply to us to access or amend their own personal information. A person is allowed to do this if the information we hold is wrong or inaccurate, incomplete, out-of-date or misleading.

Any request for access or amendment must be sent to the Information Privacy Coordinator, who can be contacted by emailing **rti&ip@ewoq.com.au** or calling **1800 662 837**, or writing to:

IP Coordinator, Energy and Water Ombudsman Queensland

PO Box 3640

SOUTH BRISBANE BC QLD 4101

What to do if you are unhappy with a decision about your personal information

If you believe that your personal information has not been handled in accordance with the IP Act, you may make a complaint to us. We will respond to that complaint in accordance with our complaint processes. Further information on EWOQ's Complaint Management Process is available on our website: **www.ewoq.com.au**.

The complaint should be made within six months from the date when the breach was suspected to have occurred.

Privacy complaints made to EWOQ must:

- give your address where we can forward notices under the IP Act;
- include certified identification;
- provide particulars of the complaint; and
- be forwarded to the contact detailed above.

Complaints will be acknowledged in writing within 14 days from the date on which the complaint is received and processed within 45 business days.

Where a longer period of time is required to finalise a complaint, we will contact the complainant to attempt to negotiate an extension of time. On completion, we will inform the complainant of our decision, including any remedies appropriate to resolve the complaint.

If a complainant does not agree with our decision or has not received a decision from us after 45 days from the date the complaint was made, they may take the complaint to the Office of the Information Commissioner (OIC). Complaints to the OIC must be in writing. More information about the Information Commissioner's privacy complaints process is available at: **www.oic.qld.gov.au/about/privacy/privacy-complaint-form**.

Useful links

- *Public Sector Act 2022*
- *Public Sector Ethics Act 1994*
- *Public Interest Disclosure Act 2010*
- *Right to Information Act 2009*
- *Information Privacy Act 2009*
- *Privacy Act 1988 (Cth)*
- *Public Records Act 2023*
- *Crime and Corruption Act 2001*
- *Energy and Water Ombudsman Act 2006*
- *Human Rights Act 2019*
- *Energy and Water Ombudsman Regulation 2007*
- Queensland Public Service Code of Conduct
- Queensland Public Service values and conduct
- Office of the Australian Information Commissioner (OAIC)

Useful references

- IPOLA Guideline - Key privacy concepts and sensitive information
- IPOLA Resource – Privacy Impact Assessment (PIA) Risk Consideration Resource
- IPOLA Resource – Privacy Impact Assessment (PIA) Threshold Assessment Form
- IPOLA Resource – Privacy Impact Assessment (PIA) Report Template
- IPOLA Guidelines | Office of the Information Commissioner Queensland