Minimising Personal Information Held

Strategies to mitigate the risk of privacy breaches

Report No. 1 to the Queensland Legislative Assembly for 2024-25

Copies of this report are available on our website at www.oic.qld.gov.au and further copies are available on request to:

Office of the Information Commissioner
Level 11, 53 Albert Street, Brisbane, Qld 4000
PO Box 10143, Adelaide Street, Brisbane, Qld 4000

Phone +61 7 3234 7373 or Freecall 1800 OIC QLD (1800 642 753)
Email administration@oic.qld.gov.au
Web www.oic.qld.gov.au

ISBN: 978-0-6456316-7-8

Office of the Information Commissioner
Queensland

December 2024

The Honourable Patrick Weir MP
Speaker of the Legislative Assembly
Parliament House
George Street
Brisbane QLD 4000

Dear Speaker

I am pleased to present an audit report, *'Minimising Personal Information Held: Strategies to mitigate the risk of privacy breaches',* prepared under section 135 of the *Information Privacy Act 2009* (Qld).

The report details an audit of Urban Utilities' practices for collecting and disposing of its residential customers' personal information.

The report makes specific recommendations to Urban Utilities and also a general recommendation that applies to all Queensland government agencies in relation to good information practices, namely, the importance of agencies:

- reviewing all information holdings and systems that contain personal information
- assessing the privacy risks of those holdings and systems
- ensuring agencies collect the minimal amount of personal information required, and
- implementing appropriate information disposal procedures.

In accordance with subsection 193(5) of the *Information Privacy Act 2009* (Qld), I request that you arrange for the report to be tabled in the Legislative Assembly.

Yours sincerely

Joanne Kummrow
Information Commissioner

Table of contents

Summary

As members of the community, we all require services from government agencies at some time. For example, we may apply for a fishing permit or want a copy of a birth certificate. Our children could be enrolled in state schools, or we may have to be admitted into a public hospital.

Every day, government agencies collect and hold our **personal information** to carry out their roles in serving Queenslanders. It might be as simple as checking our personal details, such as our name, address and date of birth, to renew a driver's licence. There could also be more complex reasons and extra personal information is required, for example, when the police are investigating an incident.

It does not mean that government agencies need to collect all our personal information or that they can hold on to it indefinitely. Collecting more information than necessary and not disposing of it when it is no longer required increases the risk of a **privacy breach**, including the risk of unauthorised access, use, disclosure, and/or loss of personal information, whether intentional or accidental.

The community expects that government agencies collect our personal information responsibly and fairly, and keep it safe. Agencies must meet their legislative and privacy obligations under the *Information Privacy Act 2009* (Qld) and the information privacy principles.

Privacy breaches can, and do, have serious consequences for affected individuals, the community and agencies. In its *Data breach preparation and response* guide,[1] the Office of the Australian Information Commissioner states:

> *Individuals whose personal information is involved in a data breach may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.*

For government agencies, a privacy breach involving personal information collected and held by government can impact public trust in government and undermine the ability of agencies to carry out and deliver important public services.

1 Office of the Australian Information Commissioner, 2019, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988* (Cth), https://www.oaic.gov.au/__data/assets/pdf_file/0023/214637/NDB-Team-Data-Breach-Preparation-and-Response-guide-June-2024.pdf. Accessed 5 November 2024.

Agencies can adopt various strategies to mitigate risks of privacy breaches. The simplest, and perhaps easiest, strategies are to collect the minimal amount of personal information required and not to keep it for longer than necessary.

The Office of the Information Commissioner audited Urban Utilities to determine whether the agency adequately manages its privacy risks and obligations by minimising the amount of customer personal information it collects and holds.

Conclusions

Urban Utilities manages its privacy risks by only collecting the personal information it requires to deliver services to its residential customers. This includes collecting additional personal information in specific circumstances, for example, the financial details of a customer who elects to pay by direct debit.

Urban Utilities disposes of most of its residential customers' personal information when it is no longer required. The agency has a disposal framework and robust processes for its billing system. The framework is generally good, but it could be more robust and better integrate with all Urban Utilities' systems.

Urban Utilities takes its privacy and records management responsibilities seriously and is committed to comply with its obligations. An internal audit on aspects of the agency's privacy management framework, conducted in 2022, is evidence of this commitment. Another example is the additional protection mechanisms put in place for some personal information holdings. They include restrictions and flags placed on specific customer accounts.

Key findings

Urban Utilities uses several systems and platforms to collect and hold the personal information of its residential customers. It generally only collects and holds the names, addresses and contact details of its customers.

The information collected is fundamentally tied to the process or reason for the collection, which is primarily to invoice the customer. Urban Utilities also records interactions, such as enquiries, with customers in its Customer Relationship Management (**CRM**) system.

When there is a change of ownership for a property serviced by Urban Utilities, the agency receives some personal information from '*Form 24 - Queensland Titles Registry*

Property Information Transfer'.[2] The transfer process populates data fields in Urban Utilities' billing and CRM systems.

Individuals may experience different customer journeys with Urban Utilities depending on their circumstances. For example, some customers require dialysis treatment at their home. They rely on uninterrupted water supply.

For these customers, Urban Utilities collects additional personal information but no more than it needs to assess the need for uninterrupted water supply. It is a good and well-planned strategy to mitigate privacy risks.

Urban Utilities' *Information Privacy Policy*, *Privacy Management Framework*, *Lawful and Defensible Destruction of Records Procedure*, and the *General Retention and Disposal Schedule*, set the framework for information disposal. The *Lawful and Defensible Destruction of Records Procedure* is a good foundational document, but high level.

The agency has a *Data Disposal Procedure* specific to its billing system. The procedure captures all aspects of the process. We found that Urban Utilities' disposal practices for its billing system are robust, clear and comprehensive.

Urban Utilities has developed a clear schedule for the retention and disposal of customer information held in its CRM. As the CRM was rolled out in 2019, the personal information held in this system is not yet due for disposal.

There is an opportunity for Urban Utilities to implement a robust disposal procedure for the CRM before the seven-year retention trigger.

Urban Utilities' disposal practices for its other systems and records are not as well advanced, although the agency is taking steps to manage the information and privacy risk.

For example, like most agencies, Urban Utilities holds physical records. Many are legacy records from water functions and operations before Urban Utilities was established in 2010. At the time of the audit, there were approximately 8000 boxes of physical records.

Agencies need good internal controls to make sure that the digital copies of records are accurate, complete and meet retention obligations before they dispose of hard copy records. We found that Urban Utilities clearly documents when and how it disposes of physical records.

2 A copy of the form is available at https://www.titlesqld.com.au/wp-content/uploads/2021/05/titles-form-24.pdf. Accessed 7 November 2024.

Urban Utilities stores recordings of its calls with customers. The personal information collected during the calls varies, depending on the parties as well as the content of the discussion.

However, there is currently no set period for retention and disposal of these recordings. This represents a risk to Urban Utilities and its customers' personal data contained in the recordings.

The internal audit conducted in 2022 gave Urban Utilities the opportunity to strengthen its privacy practices, for example by setting retention periods for personal information and regularly reporting on privacy to the Executive and the Board. Other improvement opportunities identified in the audit report include formalising and rolling out a privacy impact assessment methodology and involving the privacy officer in regular risk reviews.

Recommendations

Recommendation 1

The Information Commissioner recommends that Urban Utilities, within the next three years but before customer personal information held in the customer relationship management system is due for disposal:

a. implements a procedure for disposal of personal information held within this system

b. documents its disposal activities from the system when due, for example, completes destruction certificates.

Recommendation 2

The Information Commissioner recommends that Urban Utilities, within the next six months:

a. identifies its key systems that contain residential customers personal information

b. undertakes privacy risk assessments of those systems; and

c. provides the Office of the Information Commissioner with the results of the risk assessments.

Recommendation 3

The Information Commissioner recommends that Urban Utilities, if the risk assessment identified in Recommendation 2 indicates a privacy risk, within three years:

a. implements a procedure for disposal of personal information held within the relevant system; and

b. documents its disposal activities when due, for example, completes destruction certificates.

Recommendation 4

The Information Commissioner recommends that Urban Utilities provides to the Office of the Information Commissioner every six months updates and supporting documentation to demonstrate its progress in implementing Recommendations 1 and 3 and its *Customer Information Lifecycle* program.

Recommendation 5

The Information Commissioner recommends that all Queensland government agencies:

a. identify their key information holdings and management systems (both in hard copy and digital form) that contain personal information

b. assess the privacy risks of those holdings and systems

c. if the assessments identify privacy risks, implement risk mitigation strategies such as collecting the minimal amount of personal information required

d. implement appropriate information disposal procedures, including:

   (i) a procedure for disposal of personal information held within the system; and

   (ii) document disposal activities when due, for example, complete destruction certificates.

1 Context

In Queensland, the *Information Privacy Act 2009* (Qld) provides a framework to secure individuals' personal information[3] and protect their privacy. Agencies must comply with the information privacy principles (**IPP**) and legislative requirements of the Act when they collect and handle personal information. They should also ensure compliance with other pertinent information management and data security frameworks. These include the *Public Records Act 2002*,[4] relevant retention and disposal schedules and information security, access and use policies, standards and guidelines.[5]

For example, under IPP1, agencies must not collect personal information unless it is necessary to fulfil the purpose and directly related to the function of the agency. And, under IPP4, agencies must protect documents containing personal information against loss, unauthorised access or disclosure and any other misuse. These are strict obligations that the *Information Privacy Act 2009* (Qld) places on how an agency handles personal information. This means that agencies need to consider what they collect and how it is managed.

Government agencies should also build privacy protections into systems and practice design upfront. This embeds a 'privacy by design' approach into agency practices.

It is critical that government agencies collect and dispose of personal information in an accountable and transparent way. Agencies need to outline why they need the personal information and whether it is necessary for their functions. They also need to discard the information at the end of its lifecycle.

All government agencies can adopt strategies to mitigate privacy risk at various stages of the information's lifecycle. **Figure 1** identifies these stages.

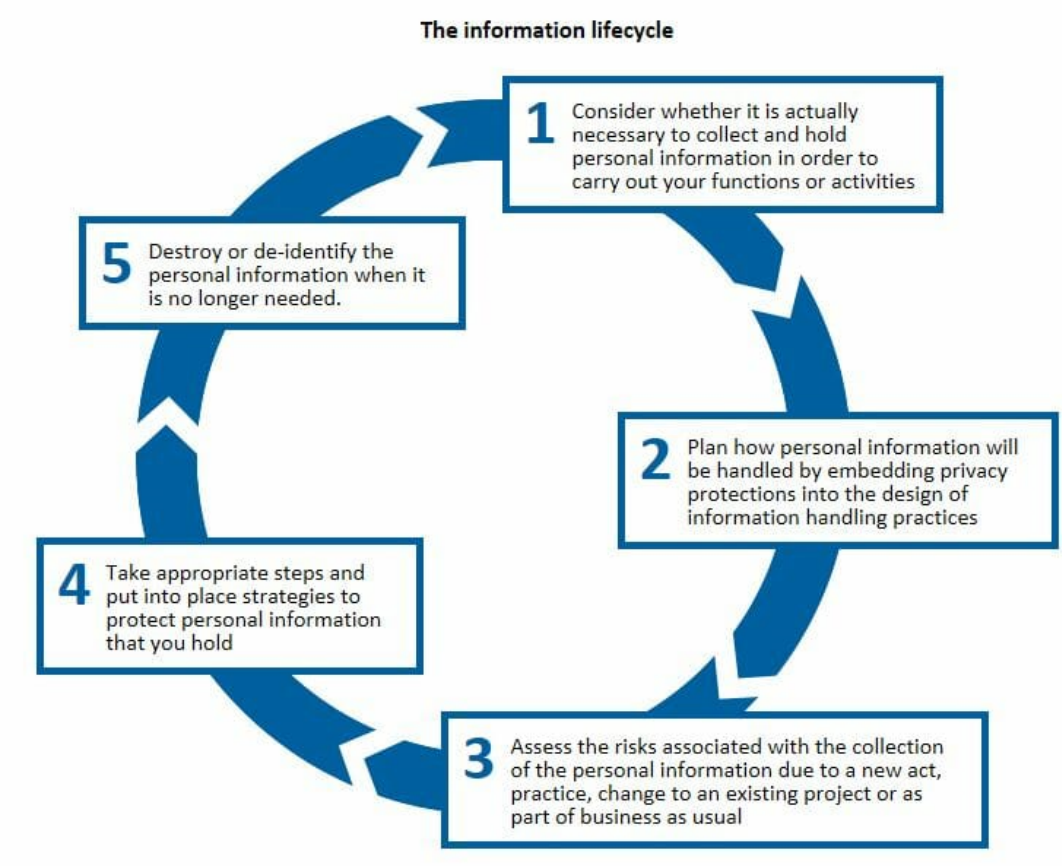
3 Section 12 of the *Information Privacy Act 2009* (Qld) defines personal information: *'Personal information is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'*

4 A new *Public Records Act 2023* (Qld) comes into effect on 5 December 2024.

5 Including for example *Information access and use policy (IS33);* and *Information security policy (IS18:2018).* Available at https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines.

Figure 1

Securing personal information



Source: Office of the Australian Information Commissioner, available at: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/guide-to-securing-personal-information.

Each stage in the lifecycle of personal information is critical to risk management. This audit focussed on two distinct phases:

- minimising what personal information is collected (phase 1)
- disposing of personal information when no longer required (phase 5).

We assessed one Queensland government agency's practices for collecting and disposing of its customers' personal information – Queensland Urban Utilities (**Urban Utilities**).

Urban Utilities

Urban Utilities is a statutory authority responsible for retail water supply and wastewater services across five local government areas in South East Queensland. This includes the councils of Brisbane, Ipswich, Lockyer Valley, Scenic Rim, and Somerset. **Figure 2** shows this geographic area.

Urban Utilities is the retail water and sewage service provider for approximately 633 300 residential properties and 30 300 commercial properties. If you live within the geographic perimeter of Urban Utilities' responsibility, it is highly likely that you receive services from Urban Utilities in some form. If this is the case, it is also probable that you or someone in your household is a customer. This means that Urban Utilities holds your personal information.

Figure 2

Urban Utilities geographic area

Source: Urban Utilities, available at: https://www.urbanutilities.com.au/about-us/who-we-are/our-geographic-area.

In 2022, Urban Utilities conducted an internal audit of aspects of its privacy management framework. It led to changes to its practices, particularly surrounding key internal systems that collect, hold and dispose of customers' personal information. These changes have been formative to how Urban Utilities manages its risks for collecting and disposing of personal information.

Audit scope and objective

The objective of this audit was to determine whether Urban Utilities adequately manages its privacy risk and obligations by minimising the amount of customer personal information it collects and holds.

We set the scope of the audit to focus on two key area of risk and examine whether Urban Utilities:

- only collects the personal information it requires to deliver services to its customers
- disposes of customer personal information when it is no longer required.

The audit scope did not include:

- Urban Utilities' practices about personal information holdings relevant to its employee and human resources functions
- implications that may arise from the *Information Privacy and Other Legislation Amendment Act 2023* (Qld).

We commenced our audit of Urban Utilities in February 2024. We met with key Urban Utilities business units and examined evidence from this time until August 2024. This report presents our findings from evidence gathered during this period.

We have, at section 3.3 of this report, referred to information Urban Utilities has subsequently provided to us.

Report structure

We structured our report as follows:

Section	Contents
Chapter 1	discusses personal information, the audit objective and scope and provides a general overview of the audited agency
Chapter 2	examines what personal information Urban Utilities collects
Chapter 3	examines how Urban Utilities disposes of customer personal information
Appendix 1	contains Urban Utilities' response and action plan

2 Collecting customer personal information

2.1 Introduction

One of the simplest, and perhaps easiest, way an organisation can reduce privacy risk is to collect minimal personal information.

Agencies should pause before collecting personal information and think about whether they need it and why. They should also be able to say how they will use the personal information. For example, an agency might think about:

- why it collects date of birth or gender identity
- whether the information is necessary to undertake the function or provide the service that it is being collected for.

Agencies must not collect personal information *'just in case'*. If they need more personal information later, agencies should collect it then, and explain why.

2.2 Conclusion

Urban Utilities only collects the personal information it requires to deliver services to its residential customers. ***What is collected*** is carefully and purposefully used.
By adopting this approach, Urban Utilities is effectively managing privacy risk.

We found that Urban Utilities tells its customers what personal information it collects and explains why it needs it and how it will use it.

In certain circumstances, Urban Utilities may collect additional personal information, for example to process direct debit payments or ensure uninterrupted water supply for critical customers.

We found that Urban Utilities has implemented protection mechanisms for some personal information holdings. They include restrictions and flags placed on specific customer accounts. This is an additional, proactive strategy to manage privacy risk.

The process to collect personal information is mostly clear, targeted and appropriate. We did find some areas for improvement to ensure that personal information holdings are accurate and up to date.

By adhering to service based collection mechanisms, Urban Utilities is not over collecting its customers' personal information.

2.3 Findings

Individuals may experience different customer journeys with Urban Utilities depending on their circumstances. This section explores what personal information Urban Utilities collects, how and for what purpose.

What is collected

Urban Utilities generally only collects and holds the names, addresses and contact details of its customers. Primarily, this information is held for billing purposes.

The agency can also collect and hold customer bank details as well as other less common types of personal information when needed or required. For example, Urban Utilities may collect more information to respond to faults and emergencies or ensure uninterrupted water supply for critical customers.

We found that Urban Utilities uses several systems and platforms to collect and hold this information. The systems are function and service driven, often linking and sharing information. It makes sense to share information across dedicated systems and not duplicate the collection processes.

Figure 3 lists 11 of the systems and platforms used by Urban Utilities. Two key systems - billing and the customer relationship management (**CRM**) – are the primary repositories of Urban Utilities' customers' personal information.

Figure 3

Urban Utilities' systems

System[6]	Use
Transfer system	Transfers data files from the Queensland Titles Office to Urban Utilities for a change of property ownership.
Billing system	Primary purpose is to enable customer billing.
CRM	Primary purpose is to record customer information and interactions with customers.
Works management systems[7]	They hold and direct work requests to Urban Utilities' maintenance and works crews.
Self-service portal (MyAccount)	Used by customers to manage their billing and account details. Registration is voluntary.

6 We have not identified the names of the individual systems.
7 Several systems are used by Urban Utilities to coordinate and manage work requests. These systems are often linked and used simultaneously.

System[6]	Use
Electronic Document and Records Management System (EDRMS)	A business-wide system containing some customer records (for example correspondence, emails).
Debt management system	Used to facilitate recovery of monies owed from overdue accounts.
Data warehouse	Used for customer surveys and research. It is a cloud-based storage system.
Mapping system	Dedicated mapping system. It is integrated with the works management systems.
Smart phone live stream system	Allows customers to use a smart phone to live stream video and pictures of faults/emergencies.
Call recordings	A system that stores recordings of calls made with Urban Utilities. Urban Utilities' call centre is the primary user of this platform.

Source: Office of the Information Commissioner.

We examined what personal information each system collects and holds.

Figure 4 identifies what personal information Urban Utilities may collect and hold in these systems.

Figure 4

Personal information held in systems

Customer personal information		
Name	Notes	Social media
Address	Class codes[8]	Related[9]
Phone	Account balances	Account history
Email	Banking details	Free text
Fax	Images	Call recordings
Customer reference numbers	Billing details	

Source: Office of the Information Commissioner.

8 This would include classification as a critical customer.
9 Related customers and properties.

The personal information held in Urban Utilities' two key systems, billing and CRM, is generally limited. All details held across Urban Utilities' systems are appropriate and necessary so that it can provide the relevant services and products to its customers.

How the personal information is collected

Generally, Urban Utilities collects its customers' personal information in two ways:

- from the Queensland Titles Office
- directly from its customers.

The information collected is fundamentally tied to the process or reason behind the collection.

We looked at what happens when a person:

- becomes an Urban Utilities customer following a **change of ownership**
- is classified as a **vulnerable customer**
- relies on uninterrupted water supply for **dialysis**
- reports a **fault or emergency**.

When a person first buys a property serviced by Urban Utilities, they become a customer. Their journey starts with a **change of ownership**. In the area serviced by Urban Utilities, there are about 50 000 to 60 000 of these dealings each year.

Urban Utilities receives some personal information from '*Form 24 - Queensland Titles Registry Property Information Transfer*'. This information is limited - it includes names, addresses, phone numbers and email addresses. The information transfer process populates data fields in Urban Utilities' billing and CRM systems. The agency needs this information mostly for billing.

Urban Utilities writes to its customers following a change of ownership. It tells them how it can collect their personal information and how it will use the information. This is a good opportunity and way that Urban Utilities explains its practices when handling personal information. It is an upfront and clear approach.

About 45 percent of change of ownership dealings are fully automated through a clear and good process. Full automation occurs when the system creates a new customer record. The process is well planned and executed.

Urban Utilities processes the remaining dealings manually. This happens when there is incorrect or insufficient data in the files it receives. For example:

- a phone number is the vendor's and not the buyer's
- the buyer provides the address of where they are living at the time of the dealing, but then moves
- the details on the form are those of the conveyancer, not the buyer
- there is more than one buyer and it is difficult to confirm accurate contact details for each party.

Urban Utilities told us that it is liaising with the Queensland Titles Office to discuss the process and improve the accuracy of the information for data integrity.

The manual process follows a clearly documented procedure to verify the identity of customers. It includes matching and transcribing customer personal information.
If there is any doubt as to an apparent match, Urban Utilities will err on the side of caution and create a new customer. This mitigates some risk.

However, because the process is manual, it lends itself to risk through human error.

Urban Utilities collects limited, if any, additional personal information for its **customers classed as vulnerable**. It means that Urban Utilities is not collecting more information, particularly information that may be sensitive, than it requires. This is a proactive and good mitigation strategy.

Urban Utilities has implemented additional protection mechanisms for some personal information holdings. They include restrictions and flags placed on specific customer accounts. It means that only designated staff and business units may access these records.

In certain circumstances, the following may appear in Urban Utilities' CRM:

The agency has also developed and implemented clear internal practices to mitigate risk to the security and protection of the personal information of some particularly

vulnerable classes of customers. For example, training instructions for Urban Utilities call centre staff include:

> *IMPORTANT: Never Provide Contact Details to Customers, always obtain. If customer asks what we have always advise them they need to tell us. Never hint what a billing address could be by providing customers the suburb.*

Some Urban Utilities customers require **dialysis** treatment at their home. They rely on uninterrupted water supply.

For these customers, Urban Utilities collects more personal information than usual. At a system level, they are visibly classed as a *critical customer.* They need to complete a particular form that includes medical information and confirmation that Queensland Health has registered the customer to have haemodialysis treatment at home. Urban Utilities also collects correspondence from a doctor confirming the treatment.

Urban Utilities does not collect more than it needs to assess the need for uninterrupted water supply. It is a good and well-planned strategy to mitigate risk to its personal information holdings for these types of customers.

Urban Utilities can require some more personal information to deal with reported **faults or emergencies**, whether it be from an existing customer or not. We found that what is collected is minimal, necessary and used. For example, it makes sense to request relevant contact details if a report requires a response or update. Good internal practices and procedures support the process.

3 Disposing of customer personal information

3.1 Introduction

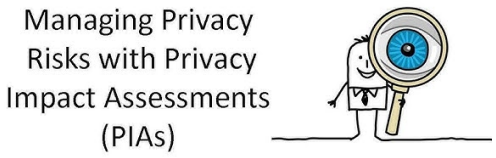
Agencies should not keep personal information for longer than required. They must consider, plan, and implement practices to destroy, and/or dispose of personal information at the end of its lifecycle.

This approach mitigates privacy risk, is consistent with Information Privacy Principle 4, and risk mitigation strategies for the lifecycle of personal information holdings identified in **Figure 1**.

In practice, this means that agencies need to:

- identify and apply prescribed retention periods for their personal information holdings
- implement retention periods in robust and detailed destruction policies and procedures
- ensure that personal information holdings are disposed of when due
- routinely revisit their processes to ensure that they are contemporary, working effectively, and up to date.

Undertaking **privacy risk assessments**[10] is a good way that agencies can identify the personal information they intend to collect, consider whether it is necessary, and address how they will manage and dispose of it. It is a valuable tool for the lifecycle of personal information.



This supports and embeds a privacy by design approach to agency practices.

10 Office of the Information Commissioner resources about privacy impact assessments are available at https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment.

3.2 Conclusion

Urban Utilities disposes of most of its residential customers' personal information when it is no longer required. The agency has a disposal framework. It is generally good, but it could be more robust and better integrate with all Urban Utilities' systems.

The billing and CRM systems hold most of the customer personal information. The billing system procedure for data disposal is robust, clear and comprehensive. It captures all aspects of the disposal process. It has identified and defined retention periods for records and customer personal information. It is a benchmark document that supports good practice.

The CRM has a well-defined retention and disposal schedule describing when different types of information are due for disposal. As Urban Utilities introduced its CRM less than seven years before the audit, there is not yet a detailed disposal procedure for this system. There is still time to implement a robust process akin to that in place for the billing system.

We have not seen similar prescriptive procedures or agreed retention requirements for records held in the other Urban Utilities' systems. This means that the personal information collected may be retained for longer than required and not destroyed within an appropriate time, if at all.

This increases the privacy risks to Urban Utilities and its customers. The agency has recognised the risk. For example, it has started to deal with legacy hard copy records.

3.3 Findings

Information disposal framework

Urban Utilities understands its privacy obligations and is committed to comply with record retention laws. It demonstrates this commitment through its *Information Privacy Policy* and *Privacy Management Framework* that support disposal activities.

Urban Utilities' *Lawful and Defensible Destruction of Records Procedure* applies to each of the systems or platforms that hold Urban Utilities' customers' personal information. The procedure's purpose is to make sure that Urban Utilities complies with the Queensland State Archive directives about disposal of records. This includes applying, and complying with, the *General Retention and Disposal Schedule.*

The *Lawful and Defensible Destruction of Records Procedure* is a reasonably good foundational document. However, it is high level. While it outlines how Urban Utilities

develops and implements plans for records disposal, it is not a procedure for managing the disposal of records and information from specific Urban Utilities' systems.

In November 2024, Urban Utilities reported that it had started a *Customer Information Lifecycle Program*. This program will examine, amongst other things, how Urban Utilities manages its customers' personal information during its lifecycle - from acquisition, storage, maintenance, use and disposal. Data cleansing activities and system enhancements are critical features of the program.

Urban Utilities said that the program is currently in its solution design phase. It reports that:

> *In relation to the timeline for delivery for the broader Customer Information Lifecycle Program, we will be in a position to commit to a timeline within 3 months of the date the report is tabled in Parliament.*

Because of the synergies between the program and our findings, and to avoid duplicating effort, we have set a longer than usual timeframe to implement our recommendations. Urban Utilities is to report regularly to our office on its progress in implementing the recommendations.

Key systems

Billing

Urban Utilities has a documented *Data Disposal Procedure* for the disposal of data held in its billing system, including its customers' personal information. The procedure captures the practical and technical steps for authorised and designated staff to conduct data disposal actions. The agency undertakes this process every quarter.

Most Urban Utilities customer personal information held in this system carries a seven-year retention period. There is one exception - direct debit information, which is one year after direct debit no longer is used. These retention periods accord with obligations prescribed by the *General Retention and Disposal Schedule*.

The procedure also requires a record of destruction activities. We found clear evidence that Urban Utilities regularly disposes of, and documents, customer personal information in its billing system.

Urban Utilities' disposal practices for its billing system are robust, clear and comprehensive. The procedure captures all aspects of the process; they are effectively actioned in practice.

Customer relationship management system (CRM)

Urban Utilities has developed and recorded a schedule for the retention and disposal of customer information held in its CRM. It is clear and comprehensive. The schedule identifies when the personal information held in its CRM will be due for disposal. This is mostly a seven-year retention period and, as with the billing system, the retention periods accord with obligations prescribed by the *General Retention and Disposal Schedule*.

Urban Utilities implemented the CRM in 2019. As a result, customer personal information held in this system is not yet due for disposal. Urban Utilities has determined when different types of information are due for disposal, but has not yet decided how it will dispose of the information.

There is an opportunity for Urban Utilities to implement a robust procedure before the seven-year retention trigger to capture and specify how it will dispose of personal information.

Recommendation 1

The Information Commissioner recommends that Urban Utilities, within the next three years but before customer personal information held in the customer relationship management system is due for disposal:

a. implements a procedure for disposal of personal information held within this system
b. documents its disposal activities from the system when due, for example, completes destruction certificates.

Other records and systems

Urban Utilities' disposal practices for its other systems and records are not as well advanced. For example, unlike for the billing and CRM systems, we did not find similar prescriptive procedures, mapping or agreed retention requirements for personal information held in the other Urban Utilities' systems or platforms.

The nature and design of many of Urban Utilities' systems that we looked at means that personal information can shared between these systems. There are improvement opportunities for Urban Utilities to make sure that practices are consistent and embedded. We looked at some these and identified challenges.

Hard copy records

Like most agencies, Urban Utilities holds physical records. At the time of our audit, there were approximately 8 000 boxes in storage containing paper documents, microfilms, CD Roms, and other records. Some of these records likely contain personal information.

Urban Utilities confirmed that 75 percent of these boxes are historical records. Legacy records include documents from water functions and operations before Urban Utilities was established in 2010. We did not review or asses these boxes and documents. However, it is highly probable that many records will be past their retention period.

To properly manage the disposal of physical records, agencies need good quality assurance and risk assessment checks. This includes making sure that digital copies of records are accurate, complete and meet retention obligations before disposing of hard copy records. We found that Urban Utilities clearly documents when and how it disposes of physical records. This is good practice.

Urban Utilities acknowledges the ongoing challenge and is taking steps to work through the hard copy documents for disposal.

Customer surveys and research

Like most service and supply operations, Urban Utilities undertakes market research to survey its customers. It often engages third party companies to carry out those activities and uses a data warehouse to hold and provide information to these companies.

The personal information in the data warehouse comes from Urban Utilities systems or platforms such as the CRM. This information is limited. It generally includes only details necessary to contact the customer.

This personal information is not retained indefinitely:

- Urban Utilities reports that this personal information is no longer available in the data warehouse when removed from the source system. This means, for example, that when the personal information is no longer held in the CRM it will not be in the data warehouse.
- According to the *Client Privacy Protection Protocol* we examined, customer personal information will be deleted by the third party engaged within three months of completion.

Collectively, these are both good mitigation strategies.

However, there is some room to strengthen the process. At the time of our audit, Urban Utilities did not receive confirmation from the third party that personal information had been deleted within the timeframe agreed to. Urban Utilities is now taking steps to embed deletion confirmation into its processes.

Smart phone live stream system

This is a tool that allows callers to live stream video and pictures of faults and emergencies using their smart phones. It allows Urban Utilities to connect with the caller without physically travelling to the site. It is a valuable tool for Urban Utilities.

During the interaction with the caller, the agent handling the call can take snapshots from the live stream. The agent can attach these images to the work request in the mapping system to allow field crew to view the footage.

However, images and recordings may inadvertently capture other personal information (of the caller or third parties) not relevant to the fault or emergency. This generates some risk that Urban Utilities collects more personal information than it requires.

We found that Urban Utilities introduced privacy impact assessments into its business practices in July 2021. It had not undertaken a privacy impact assessment for this system at the time of our audit. This represents a risk to Urban Utilities and its customers.

Call recordings

Urban Utilities stores recordings of its calls with customers. The personal information collected during the calls varies, depending on the parties as well as the content of the discussion.

However, there is currently no set period for retention and disposal of these recordings. This represents a risk to Urban Utilities and its customers.

Recommendation 2

The Information Commissioner recommends that Urban Utilities, within the next six months:

a. identifies its key systems that contain residential customers personal information
b. undertakes privacy risk assessments of those systems; and
c. provides the Office of the Information Commissioner with the results of the risk assessments.

Recommendation 3

The Information Commissioner recommends that Urban Utilities, if the risk assessment identified in Recommendation 2 indicates a privacy risk, within three years:

a. implements a procedure for disposal of personal information held within the relevant system; and

b. documents its disposal activities when due, for example, completes destruction certificates.

Recommendation 4

The Information Commissioner recommends that Urban Utilities provides to the Office of the Information Commissioner every six months updates and supporting documentation to demonstrate its progress in implementing Recommendations 1 and 3 and its *Customer Information Lifecycle* program.

Recommendation 5

The Information Commissioner recommends that all Queensland government agencies:

a. identify their key information holdings and management systems (both in hard copy and digital form) that contain personal information

b. assess the privacy risks of those holdings and systems

c. if the assessments identify privacy risks, implement risk mitigation strategies such as collecting the minimal amount of personal information required

d. implement appropriate information disposal procedures, including:

   (i) a procedure for disposal of personal information held within the system; and

   (ii) document disposal activities when due, for example, complete destruction certificates.

4 Appendix - Agency response and action plan

GPO Box 2765
Brisbane QLD 4001
(07) 3855 6000

Paul.arnold@urbanutilities.com.au

27 November 2024

Ms Joanne Kummrow
Information Commissioner
Office of the Information Commissioner

By email

Dear Ms Kummrow,

Audit Report – Minimising personal information held

I refer to your correspondence of 22 November 2024 attaching the final report of the audit into Urban Utilities' handling of its residential customers' personal information.

We welcome the findings and the opportunity the audit has given us to reflect upon and improve our privacy practices. I appreciate the recognition of the work that we have done to date, which demonstrates that we take our privacy responsibilities and obligations seriously and are committed to protecting the personal information of our customers.

We accept the need to dispose personal information from our customer systems and the need to continue the broader privacy work of our Customer Information Lifecycle Program, which commenced last year in November 2023. Given the scale of the work involved across multiple systems and processes, I acknowledge the extended timeframes reflected in your office's recommendations.

We thank your staff for their professional and constructive approach to the audit, and we look forward to continuing to work with your office as we deliver on the enclosed Action Plan.

Yours sincerely

Paul Arnold
Chief Executive Officer
Urban Utilities

General Enquiries **13 26 57**
Faults and Emergencies **13 23 64**
urbanutilities.com.au

ABN 86 673 835 011

Action Plan – Urban Utilities

Recommendation	Urban Utilities response and proposed action
Recommendation 1 The Information Commissioner recommends that Urban Utilities, within the next three years but before customer personal information held in the customer relationship management system is due for disposal: a. implements a procedure for disposal of personal information held within this system b. documents its disposal activities from the system when due, for example, completes destruction certificates.	**Response**: Urban Utilities acknowledges the recommendation.
	Proposed management action: Urban Utilities will implement a procedure for disposal of personal information held within the customer relationship management system and document its disposal activities from the system.
	Nominated owner: Tracey Marshall, General Manager, Customer Experience
	Nominated completion date: December 2027
Recommendation 2 The Information Commissioner recommends that Urban Utilities, within the next six months: a. identifies its key systems that contain residential customers personal information b. undertakes privacy risk assessments of those systems; and	**Response**: Urban Utilities acknowledges the recommendation.
	Proposed management action: Urban Utilities will undertake a privacy risk assessment of systems that contain residential customers' personal information and provide the OIC with the result.
	Nominated owner: Eleanor Madden, Manager, Privacy and RTI

Recommendation	Urban Utilities response and proposed action
c. provides the Office of the Information Commissioner with the results of the risk assessments.	**Nominated completion date:** April 2025
Recommendation 3 The Information Commissioner recommends that Urban Utilities, if the risk assessment identified in Recommendation 2 indicates a privacy risk, within three years: a. implements a procedure for disposal of personal information held within the relevant system; and b. documents its disposal activities when due, for example, completes destruction certificates.	**Response**: Urban Utilities acknowledges the recommendation.
	Proposed management action: Urban Utilities will implement a procedure for disposal of personal information and document its disposal activities from the systems identified via the privacy risk assessment.
	Nominated owner: Tracey Marshall, General Manager, Customer Experience
	Nominated completion date: December 2027

Recommendation	Urban Utilities response and proposed action
Recommendation 4 The Information Commissioner recommends that Urban Utilities provides to the Office of the Information Commissioner every six months updates and supporting documentation to demonstrate its progress in implementing Recommendations 1 and 3 and its Customer Information Lifecycle program.	**Response**: Urban Utilities acknowledges the recommendation.
	Proposed management actions: 1. Urban Utilities will provide the OIC with a roadmap for the Customer Information Lifecycle Program within 3 months. 2. Urban Utilities will provide six monthly updates and supporting documentation to the OIC to demonstrate its progress in implementing Recommendations 1 and 3 and the Customer Information Lifecycle Program.
	Nominated owner: Eleanor Madden, Manager, Privacy and RTI
	Nominated completion date: 1. Roadmap for the Customer Information Lifecycle Program: March 2025. 2. Ongoing six-monthly updates: commencing from June 2025