

Information Privacy: Complaints and Breaches Investigation Policy

Created: November 2019



Queensland
Government

1. Policy Statement

The Department of Justice and Attorney-General (DJAG) values and protects the personal information of clients, customers and employees collected in accordance with its business needs in the delivery of government functions and services. DJAG is committed to managing complaints made under the [Information Privacy Act 2009](#) (IP Act) or complaints made about the management of tax file numbers (TFNs) and tax file number (TFN) information under the [Privacy Act 1988 \(Cth\)](#)¹ (Privacy Act) in an accountable, transparent, timely and fair manner.

DJAG recognises the importance of providing an efficient and client focussed approach to the privacy complaint handling process as integral to effective customer service and does so in accordance with legislative requirements under the IP Act.

DJAG values the benefits of effective privacy complaint handling as it contributes to the development and implementation of improved work practices and service delivery across the department. Accordingly, DJAG encourages a proactive approach to complaints management. This includes the consideration of human rights issues in all complaints (see paragraph 6 below).

The *Information Privacy: Complaints and Breaches Investigation Policy* (this policy) and the [Information Privacy: Complaints and Breaches Investigation Procedure](#) will be published on:

- DJAG's intranet; and
- DJAG's publication scheme.

NOTE: If you have any questions regarding a privacy complaint, contact Right to Information (RTI) and Privacy, DJAG on (07) 3738 9893, or via email at privacy@justice.qld.gov.au.

2. Objectives

This policy sets out matters related to privacy complaints and investigations managed by Right to Information (RTI) and Privacy or Legal Advice and Advocacy. The objectives of this policy are to ensure:

- transparent, accountable and responsive management of privacy complaints;
- consistency in the approach to privacy complaints and investigations;
- privacy complaints and investigations are handled effectively;
- the rights of complainants and respondents are protected; and
- support and provision of a policy framework for the [Information Privacy: Complaints and Breaches Investigation Procedure](#).

¹ In particular, see [section 26WE\(1\)\(d\) Privacy Act \(Cth\) 1988](#) and the [Commonwealth \(Tax File Number\) Rule 2015](#).

3. Principles

The complaint management principles underlying this policy reflect the [AS/NZS 10002:2014 Guidelines for complaint management in organisations](#) (the Guidelines), and [section 219A of the Public Service Act 2008](#) – which prescribes the need for a complaints management system in all Queensland Government agencies. This policy is to be read in conjunction with [Information Privacy: Complaints and Breaches Investigation Procedure](#); [Information Privacy Breach and Complaint Assessment Triage](#); and DJAG's [Client Complaints Management Policy](#).

DJAG is committed to the following complaints management principles in managing privacy complaints:

- the privacy complaints process is free and accessible and supports natural justice for all individuals with no detriment associated with making a complaint.
- information for individuals on how to lodge a privacy complaint and how their complaint will be managed will be available to individuals.
- provision of information outlining what types of outcomes can be achieved through the privacy complaints process.
- the right to have an authorised agent to act on behalf of the individual making the privacy complaint.
- communication with individuals about the progress of their privacy complaint.
- providing individuals with an explanation of the decision, any recommendation and review options available if they do not agree with the outcome.
- if relevant, the continuous improvement of service delivery and DJAG's procedures and practices.
- responding to complaints in a respectful, fair and objective manner.
- adhering to legislative timeframes when investigating complaints.
- adopting a systems approach to privacy complaints which places a focus on reviewing practices, processes, policies, and procedures to assess whether amendments to existing practices or the development of new practices are required to prevent further breaches.
- privacy complaints (with the exception of technical low-level privacy breaches), written or verbal, are to be sent or referred to RTI and Privacy, with DJAG to investigate and manage the complaints in accordance with this policy; [Information Privacy: Complaints and Breaches Investigation Procedure](#); and [Information Privacy Breach and Complaint Assessment Triage Form](#).
- ensuring that technical low-level privacy breaches are managed in accordance with the [Management of Technical \(low level\) Privacy Breaches Procedure](#). This procedure provides guidance to business units when dealing with technical low level privacy breaches. Examples of technical low level privacy breaches could be, but are not limited to:

- a document being attached to an incorrect system account, where no reliance or decision has been made on the incorrect information;
 - information regarding an officer attached to another officer's hardcopy file, provided it has not been used to support a decision; and
 - an email regarding an individual sent to an incorrect person, but still within DJAG, and where advice has been received that the email has been deleted.
- technical low level privacy breaches which have been resolved by the relevant business unit under the [Management of Technical \(low level\) Privacy Breaches Procedure](#) are still to be reported to RTI and Privacy as it needs to report and monitor cause and effect as well as trends about privacy breaches.

4. Complaint Jurisdiction and timelines

DJAG, as an agency, has obligations under the [11 Information Privacy Principles \(IPPs\) contained in schedule 3 of the IP Act](#). Failure to comply with these principles will potentially lead to a privacy breach with consequences that can range from being insignificant to significant (which may include an order for compensation made by QCAT).

[Section 164\(1\) of the IP Act](#) outlines the meaning of a 'privacy complaint'. The elements of a 'privacy complaint' are as follows:

- a complaint;
- by an individual;
- about an act or practice by a relevant entity;
- in relation to the individual's own personal information; and
- that relevant entity breached its obligations under the IP Act to comply with-
 - (a) the privacy principles; or
 - (b) an approval under [section 157](#).

A 'relevant entity' means an agency, in relation to documents of the agency; or a bound contract service provider, in relation to documents held by the bound contracted service provider for the purposes of performing its obligations under a service arrangement.

A privacy complaint can be made by a client, customer, or an officer in their capacity as an employee in relation to their own personal information. An agent may make a privacy complaint or act on behalf of another individual². However, an agent acting on behalf of the complainant must provide DJAG with evidence of their authority from the complainant to act on the complainant's behalf.

If the complaint relates to a breach of Privacy Act [Privacy \(Tax File Number\) Rule 2015](#), refer to [Data Breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 \(Cth\), Part 4: Notifiable Data Breaches \(NDB\) scheme, Office of the Australian Information Commissioner \(OAIC\)](#). DJAG, as a TFN recipient, must comply with the mandatory data breach notification obligations under the [Privacy \(Tax File Number Rule\) 2015](#), a legislative instrument made under [section 17 of the Privacy Act](#).

² [Section 196 of the IP Act](#).

Complaints received which do not relate to an alleged breach of the [11 IPPs](#) or do not relate to the management of TFNs or TFN information will be referred to the relevant business unit for action in accordance with DJAG's [Client complaint management policy](#) the *Employee complaints policy* or the [Public Interest Disclosure Policy](#).

A privacy complaint is valid from the date it satisfies the meaning of 'privacy complaint' in [section 164\(1\) IP Act](#) irrespective of which business unit received it within DJAG - that is the complaint is by a person about an act or practice of DJAG in relation to that person's personal information and is an alleged breach of DJAG's obligation under the IP Act to comply with the IPPs

All privacy complaints, (with the exception of technical low level privacy breaches), written or verbal must be sent or referred to RTI and Privacy (privacy@justice.qld.gov.au) immediately upon receipt of the complaint. The agency has 45 business days in which to respond to the complainant as implied in [section 166\(3\)\(b\) of the IP Act](#).

If 45 business days have elapsed since a privacy complaint was made and the complainant has not received a response from the department, or if the complainant received a response, but does not consider it to be an adequate response, the complainant may refer the matter to the Office of the Information Commissioner (OIC). Information about the OIC's privacy complaint processes is available at <https://www.oic.qld.gov.au/about/privacy/privacy-complaints>.

Generally, a privacy complaint must be made within 12 months after the complainant became aware of the decision or action of the entity. Complaints made outside this time period may be reviewed by DJAG depending on the circumstances and merits of the matter. A privacy breach assessment report will be completed and provided as necessary to relevant management.

5. Identified Breaches

Privacy breaches must be reported and dealt with regardless of whether a complaint has been received in relation to the conduct or incident.

6. Ethical Standards, People and Engagement Branch and Information Technology Services

RTI and Privacy will consult with the Ethical Standards Unit (ESU) and/or People and Engagement Branch in instances where the initial assessment of a complaint or investigation indicates that a DJAG officer may have acted inconsistently with the [Code of Conduct for the Queensland Public Service](#), if there is alleged or suspected corrupt conduct or possible criminal activity.

If at the initial assessment stage it is considered that the privacy breach may be a result of a cyber breach, determine whether to consult with Information Technology Services (ITS) who may take action in accordance with the DJAG cyber incident response plan. If it is found that a privacy breach is a result of a cyber breach, ITS is to report to DJAG security steering committee (ITIC) and carry out mandatory reporting to the Queensland Government Chief Information Office (QGCI) under the [security incident reporting standard](#).

Any matters involving disclosures under the [Public Interest Disclosure Act 2010](#) will be referred to the Executive Director, Ethical Standards Unit as the Public Interest Disclosure co-ordinator and managed in accordance with [DJAG's Public Interest Disclosure Policy](#).

7. Human Rights

Human rights should permeate the consideration of all complaints, not just those where a breach of a human right is specifically alleged by the complainant. In identifying human rights relevant to a complaint refer to [Human Rights Portal](#). RTI and Privacy will manage complaints alleging a breach of an individual's right to privacy.

8. Complaints Management Model

DJAG's complaints management model is based on the following process:

- Internal assessment
- Internal investigation (where necessary)
- Internally facilitated resolution
- Outcome and response to a privacy breach
- Response to a privacy complainant

The steps within this model are further elaborated on in the [Information Privacy: Complaints and Breaches Investigation Procedure](#).

9. Reporting

A report by RTI and Privacy to senior management listing all current complaints and the outcome of investigations into privacy complaints is updated weekly.

Both qualitative and quantitative data is recorded and captured in the Client Management System (CMS) used by RTI and Privacy. A report can be generated upon request by business units if they wish to be informed about the number of breaches or complaints relating to their business area.

10. Authority

[Public Service Act 2008](#)

[Ombudsman Act 2001](#)

[Public Interest Disclosures Act 2010](#)

[Information Privacy Act 2009](#)

[AS/NZS 10002:2014 Guidelines for complaint management in organizations](#)

11. Related Legislation, procedures and guidelines

[Information Privacy: Complaints and Breaches Investigation Procedure](#)

[DJAG Client complaint management policy](#)

[DJAG Client complaint management handbook](#)

[Public Interest Disclosure Policy](#)

[Public Sector Ethics Act 1994](#)

[Employee complaints policy](#)

[Code of Conduct for the Queensland Public Service](#)

[Australian/New Zealand Standard AS/NZS 1002-2014 Guidelines for complaints management in organizations](#)

[Public Service Act 2008](#)

[Ombudsman Act 2001](#)

[Public Interest Disclosures Act 2010](#)

[Information Privacy Act 2009](#)

[Privacy Act 1988 \(Cth\)](#)

[Commonwealth \(Tax File Number\) Rule 2015](#)

[Human Rights Act 2019](#)