Information Privacy: Complaints and Breaches Investigation Procedure

Created: November 2019

1. Purpose

The *Information Privacy: Complaints and Breaches Investigation Procedure* has been developed to ensure consistency in investigating privacy complaints by relevant Officers in the Department of Justice and Attorney-General (DJAG).[1] It is a guide for the procedures involved in the assessment, investigation and management of privacy complaints and breaches made under the *Information Privacy Act 2009* (IP Act). This procedure is to be read in conjunction with DJAG's *Information Privacy: Complaints and Breaches Investigations Policy.*

2. Roles and Responsibilities

All privacy complaints and breaches will be assessed, investigated and managed by the relevant Officer to determine if there has been a breach of any of the 11 Information Privacy Principles (IPPs) in Schedule 3 of the IP Act. The table below sets out the definition of the title of relevant Officers involved in investigating and managing privacy complaints.

Term	Definition/Explanation
Approving Officer	The Officer who approves the classification of a privacy complaint or breach on the Information *Privacy Complaint and Breach Assessment Triage Form* (Assessment Triage Form). The Officer may also make the decision on a privacy complaint or privacy breach. This may be the Director, the Principal Advisor, the Principal Executive Officer, RTI and Privacy, or an officer from Legal Advice and Advocacy.
Assessing Officer	The Officer who assesses whether a privacy complaint or breach is valid and determines the classification level of the issue.
Investigating Officer	The Investigating Officer will usually conduct the investigation in accordance with their position responsibilities and may also be the Receiving Officer, the Assessing Officer and make the decision on a privacy complaint or privacy breach.
Receiving Officer	The Officer who receives the privacy complaint or breach, records the information in the Client Management System (CMS) and refers the file, both electronic and hardcopy to the Assessing Officer. This Officer may also be the Approving Officer.

3. Complaint Method

All privacy complaints, whether written or verbal, must be sent or referred to RTI and Privacy:

Phone	(07) 3738 9893
Fax	(07) 3738 9922
Address	Right to Information and Privacy

[1] Officers in Right to Information and Privacy, and Legal Advice and Advocacy

	Department of Justice and Attorney-General GPO Box 149 Brisbane QLD 4001 or Level 17, State Law Building 50 Ann Street Brisbane QLD 4000
Email	privacy@justice.qld.gov.au

4. Assistance and Accessibility when making a Complaint

Where an individual makes a complaint about an alleged breach of privacy and is unable to put that complaint in writing, the RTI and Privacy Officer DJAG accepting the complaint must provide the individual with assistance to make their complaint in writing. This may include transcribing the individual's complaint on their behalf. The Officer transcribing the complaint must read the complaint back to the individual to ensure that all of the information is captured correctly and send a copy of the complaint to the complainant.

If an individual has difficulty in making the complaint themselves, they may be supported by another person to make their complaint.

If an individual is from a culturally and/or linguistically diverse background, and requires a translator or interpreter, the Translating and Interpreter Service (TIS) may be used. The phone number for TIS is 131 450. For more information about using interpreters please see Translating and Interpreter Service.

Where verbal assistance is provided to an individual to enable them to make a complaint, the individual must be made aware of the following privacy notice in accordance with IPP2 of the IP Act:

The Department of Justice and Attorney-General (DJAG) is collecting your personal information from you to manage your complaint in accordance with DJAG's Privacy Complaints and Breaches Investigation Procedure. Your personal information will not otherwise be used and disclosed unless authorised or required under a law. We will manage your personal information in accordance with the Information Privacy Principles of the Information Privacy Act 2009 (Qld).

5. Privacy Complaint

Section 164(1) of the IP Act defines a 'privacy complaint'. The following list contains elements of the definition of 'privacy complaint' as outlined in the IP Act:

- a complaint;
- by an individual;
- about an act or practice of DJAG;
- in relation to the individual's **own** personal information; and
- that is a breach of DJAG's obligations under the IP Act to comply with –
  (a) the privacy principles; or
  (b) an approval under section 157.

A privacy complaint is valid from the date it complies with the requirements of section 164(1) of the IP Act, irrespective of which business unit received it within DJAG. All written

or verbal privacy complaints must be sent or referred to RTI and Privacy (privacy@justice.qld.gov.au) immediately upon receipt of the complaint.

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

Individuals who complain about matters other than privacy will be referred to DJAG's *Client complaint management policy*, *Employee complaints policy* or the *Public Interest Disclosure Policy* where relevant and advised to contact the appropriate business unit to handle their complaint.

DJAG also has responsibilities under the *Privacy Act 1988* (Cth) Privacy (Tax File Number) Rule 2015 in relation to reporting serious data breaches concerning an individual's Tax File Number (TFN) and TFN information[2].

6. Privacy Breach

Privacy breach is not defined in the IP Act, however, the Office of the Information Commissioner's (OIC) website, states:

A privacy breach occurs when there is a failure to comply with one or more of the privacy principles set out in the Information Privacy Act 2009.
Privacy breaches can occur because of a technical problem, human error, inadequate policies and training, a misunderstanding of the law, or a deliberate act. Some of the more common privacy breaches happen when personal information is lost, stolen or mistakenly disclosed (for example, a USB flash drive is lost or an email is sent to unintended recipients).[3]

7. Creating a Complaint or Breach File

When a complaint or breach notification is received with respect to personal information, including the management of TFNs or TFN information, a file is to be created in the Client Management System (CMS) and the electronic document management system (eDocs). A request for the hardcopy eDocs file must be sent to RTIAdministration@justice.qld.gov.au.

Create the *Information Privacy Complaint and Breach Assessment Triage Form* in CMS, and save it into the relevant eDocs file folder. Enter the details into the Privacy Workload Register.

Comprehensive records must be kept to demonstrate that privacy complaints and breaches are appropriately assessed, investigated and resolved. All correspondence including internal correspondence, reports and memoranda is to be filed and saved within the complaint file in eDocs or on the hardcopy file (not on both electronic and hardcopy).

Correspondence, file notes of telephone conversations, other file notes and reports are to be generated through CMS and saved in eDocs. Quarantine access to the file to ensure

[2] see *Definitions Table*
[3] Privacy breach management and notification | Office of the Information Commissioner Queensland

DJAG officers who were involved in the handling of the personal information which is the subject of the complaint or breach cannot electronically or physically access any documentation in the file.

8. Completing Part 1 of the *Information Privacy Complaint and Breach Assessment Triage Form* - Acceptance

After creating the complaint or breach file, the first part of the Assessment Triage Form must be completed by the Receiving Officer. To assist in the intake, refer to privacy complaint checklist steps 1-10 in the *Information Privacy Complaint and Breach Assessment Triage Form* and complete as follows:

a. Read through the privacy breach or complaint notification

b. Identify whether the matter is a privacy breach, privacy complaint; or a complaint relating to a TFN or TFN information and check the appropriate box shown here:

Privacy Breach	☐
Privacy Complaint	☐
TFN Breach	☐
Other	

c. Complete the basic information table based on information received in the privacy complaint or breach notification for example:

Date received by RTI and Privacy: 10 June 2017	**Date of Breach:** 6 June 2019
How was complaint submitted? email	**CMS No.:** 584239 **eDocs File Folder No.:** 2686398
Notifier / Complainant: Ms Jane Smith	
Précis: Ms Jane Smith complains that her privacy was breached by …..	

d. Complete jurisdictional questions 1 to 7 by deleting the answer which is not relevant to the notification.

e. If the matter does not relate to DJAG send the complaint/notification back to the complainant/notifier advising them that the matter is not a DJAG matter and advising them of the contact details for the relevant agency.

f. The Receiving Officer must note their name, date and signature (this can be electronic) on the second line of the *Approval Table* as per this example:

Accepted by:	Paul Doe	**Signature:** Paul Doe	**Date:** 10 June 2019

g. Email the Assessment Triage Form, and provide the eDocs folder to the Assessing Officer for further action.

9. Assessing Complaint or Breach Complexity

In assessing the privacy complaint complexity, refer to the privacy complaint checklist steps 1-10 in the Assessment Triage Form.

The level of complexity is defined on the Assessment Triage Form. It is also outlined in this procedure for additional clarity.

Minor: Assessed as having negligible risk or detriment to DJAG and/or stakeholders and/or affected individual/s in relation to non-compliance of the IP Act. Requires no investigation.

Standard: Assessed with minimal risk or detriment to DJAG and/or stakeholders and/or affected individual/s in relation to non-compliance of the IP Act. Requires no investigation or minimal investigation.

Intermediate: Assessed with medium level of risk or detriment to DJAG and/or stakeholders and/or affected individual/s in relation to non-compliance of the IP Act and may require detailed investigation.

Complex: Assessed with serious or significant level of risk or detriment to DJAG and/or stakeholders and/or affected individual/s in relation to non-compliance of the IP Act and/or *Privacy Act 1988* (Cth) Privacy (Tax File Number) Rule 2015. Immediate action required. Higher level investigation required and immediate referral to executive management. Information contains TFN information or a TFN.

Further information and examples on the types of issues that would occur under each of these criteria are outlined in the *Action and Classification Table* on the *Information Privacy Complaint and Breach Assessment Triage Form*. Please note, privacy complaints and breaches may be reclassified at any time throughout the investigation process, for example, based on investigation findings or new information from the complainant.

10. Assessing Complaint or Breach Complexity

Once it is confirmed that the complaint meets the meaning of a privacy complaint, and a file has been created, the Assessing Officer must determine the complexity of the complaint using the Assessment Triage Form as follows:

a. Read through the privacy complaint or brief/information received about a privacy breach.

b. Check the boxes for the relevant IPPs applying to the matter, based on the information available at the time of assessment.

c. Ensure the information required for the privacy complaint or breach is saved in the relevant eDocs and CMS files, and check each box once the information has been provided and recorded.

d. Use the *Action and Classification Table* on the *Information Privacy Complaint and Breach Assessment Triage Form* to determine the complexity of the alleged privacy breach. Highlight the relevant criteria using the classification colours set out in the *Action and Classification Table*.

Minor
Standard
Intermediate
Complex

e. Analyse the actions listed in the *Action and Classification Table* to determine the level of the alleged breach. If it is not clear from the list what level classification should be attributed to the alleged breach, automatically upgrade the classification to Complex which will ensure the alleged breach is managed appropriately. If the personal information subject to the alleged breach cannot be contained, the classification should automatically be upgraded to Complex due to the associated risks. For example, in relation to an alleged breach where the information was contained, Standard would be chosen.

Action and Classification Table

Action	Minor	Standard	Intermediate	Complex
Containment	Involves a use rather than a disclosure of personal information.	Limited distribution of personal information and still under the control of DJAG. Personal information has been contained.	Wider distribution of personal information and the potential for further disclosure of use.	Personal information cannot be contained OR The matter is a serious data breach relating to an individual's TFN or TFN information.

Extract from Action and Classification Table in the *Information Privacy Complaint and Breach Assessment Triage Form*

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

g. RTI and Privacy will make an initial assessment of the complaint to identify any human rights issues by referring to the Human Rights Portal. If it is identified that the complaint does have a human rights component, whether identified or not by the complainant, the complaint may be actioned by RTI and Privacy (if the complaint relates to a breach of an individual's right to privacy) or will be referred back to the business area responsible for the function being complained about, as consistent with current practice.

h. 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 Queensland Government Chief Information Office (QGCIO) under security incident reporting standard.

i. 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.

j. The Assessing Officer must identify the classification type and note their name, date and signature (this can be electronic, but preferably by hand written signature) next to "Assessed By" in the *Approval Table*. The Assessing Officer may also be the Receiving Officer.

k. The completed *Information Privacy Complaint and Breach Assessment Triage Form* must be sent to the Approving Officer. The Approving Officer must not be less senior than the Receiving/Assessment Officer.

11. Assessing a Data Breach or Complaint about the Management of an Individual's TFN or TFN information

The Assessing Officer must identify whether a TFN is involved in the data breach or complaint. If so, they must make the Approving Officer aware of the issue due to mandatory data breach notification obligations under the *Privacy Act 1988* (Cth).

Where it is clear that a TFN data breach has occurred, the Investigating Officer must follow the requirements outlined on the Office of the Australian Information Commissioner's (OAIC) website at https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify and complete a Notifiable Data Breach Form as part of their investigation.

In circumstances where it is not clear whether a TFN data breach has occurred, the Investigation Officer may be required to conduct the investigation prior to notifying the OAIC.

12. Assessment Triage Form Timeframes

The Assessment Triage Form must be submitted by the Assessing Officer to the Approving Officer within 2 business days from the date the privacy complaint or breach is received by the Receiving Officer.

The Approving Officer must approve the *Information Privacy Complaint and Breach Assessment Triage Form* within three business days from the day the Assessing Officer returns the completed *Information Privacy Complaint and Breach Assessment Triage Form* to the Approving Officer.

These timeframes may be adjusted in exceptional circumstances with the agreement of the Director, RTI and Privacy.

13. Acknowledgement of Complaint

A written acknowledgment letter of the receipt of an individual's privacy complaint will be sent to the complainant within 5 business days of receipt of their complaint by RTI and Privacy.

Complaints about issues other than privacy will be managed and referred to other areas of DJAG in accordance with DJAG's *Client complaint management policy*, *Employee complaints policy* or the *Public Interest Disclosure Policy* as appropriate, and the complainant informed.

The privacy complaint must be acknowledged using the template Acknowledgement Letter (PRV050). As outlined in DJAG's *Client complaint management handbook* which is referenced in the *Client complaint management policy*, priority will be given to clients

who are vulnerable, children and young people and in these circumstances, the complaint must be acknowledged as soon as possible.

The acknowledgement letter must:

- assure the complainant that their feedback/complaint is valued.
- define the scope of the complaint and invite the complainant to confirm the scope of the complaint as defined.
- request any further information necessary to action the complaint, outline how the complaint will be managed, including a timeframe for resolution.
- extend to the complainant the opportunity to offer a resolution of their complaint.
- provide contact details for the DJAG Officer managing the complaint.
- advise the complainant about how their personal information will be used and disclosed as part of the investigation.

A response will be provided to the complainant within 45 business days from the date the complaint becomes valid, as outlined in paragraph 5 Privacy Complaint above.

14. Investigating the Complaint or Breach

Privacy complaints will be dealt with fairly and objectively, and in accordance with natural justice principles[4]. The investigation process will be undertaken with as little formality as possible and in the spirit of collaboration, business improvement and complaint resolution. Each investigation is unique, so the order and extent of an officer's approach to each investigation may vary depending on the specific factors of the complaint or breach.

a. Identify the scope of the investigation

Examine the complaint or breach information and the Assessment Triage Form to identify the legislative issues enlivened by the complaint or breach. This will enable the Investigating Officer to gain a clear understanding of what issues fall within the scope of the investigation.

b. Resolution of a complaint

If the matter is a complaint, identify the complainant's expected outcome, and whether this can be achieved by DJAG. If the complainant has not proposed a resolution, provide the complainant with an opportunity to identify a resolution for their complaint. The types of resolutions which may be able to be achieved include:

- providing specific Officers or business units with targeted training on the IP Act or the handling of TFNs;
- a letter of apology; or

[4] Natural justice is the right to be made aware of, and respond to, information which will be used in the course of a decision which will negatively affect the person. Non-adverse information, and adverse information which will not be used to make a decision, does not necessarily have to be provided.

- a change in business practices.

Please note if the complainant requests financial compensation as a resolution, this will be a matter for the business unit to decide in consultation with Executive management and Legal Advice and Advocacy.

c. Investigation planning

Where an investigation is required, the Investigating Officer must begin planning it by identifying information to be sought from Officers and business units in order to reach a conclusion on matter. This does not need to be a formal process. There are a number of questions that the Investigating Officer may consider in order to gather information to identify whether a privacy breach has occurred.

The following is a non-exhaustive list of matters which the Investigating Officer may wish to consider when deciding on the types of information they require to reach a view on the matter:

- which business units are relevant to the alleged privacy breach.
- is the allegation about the conduct of one or more officers? If so, who are the relevant officers; and who is their line Manager?
- if DJAG officers have been identified as being able to assist an investigation by providing evidence, how can those officers be best contacted to invite them to an interview?
- immediate preservation of evidence, for example, any CCTV footage.
- the availability of interviewees.
- whether relevant supervisors or managers must also be contacted for further information or to attend an interview.
- any special access requirements that must be addressed, for example, whether access clearance is required for the Investigating Officer, recording equipment, disability services, or translation services.
- whether it is a matter which requires consultation with ESU/P&E/ITS.
- whether it is likely that the investigation process will exceed 45 business days. If so what contingency plans are in place and who needs to be notified of this?
- what evidence already exists and in which form, for example CCTV footage, photographs, documents, soft copy files, emails, and how that evidence can be obtained?
- whether external evidence is required, for instance, from another government department or a private individual.
- whether technical expertise or other expert assistance is required.

- what, if any, contingency plan can be put in place if an officer or other individual who can assist the investigation refuses or otherwise is unable to take part in an interview.

- whether evidence can be obtained by some other method, for example, by way of a written and signed statement.

- whether it appears that the matter relates to the management of TFNs or number information and, if proven, would it be a serious data breach which will trigger a mandatory data breach Notification under the *Privacy Act 1988* Privacy (Tax File Number) Rule 2015.

d. Requesting information from relevant parties

The Investigating Officer must use the approved template (PRV080) when contacting individuals relevant to the matter (including DJAG officers) to attend an interview about the alleged breach.

e. Documenting information

When information about the privacy breach or complaint is received from relevant parties, ensure that CMS is updated accordingly with the information and time spent on the matter.

A record of any interview conducted must be made. These records can be in an audio electronic form or written as contemporaneous file notes during the interview.

f. Evaluate the evidence

Once the evidence has been received from the relevant parties, determine the weight to be applied to it. The standard of proof used by DJAG is the civil standard of proof. That is, that the complaint is made out or confirmed to have more than likely occurred, based on the balance of probabilities.

g. Natural justice

All parties affected by a decision adverse to them will be afforded natural justice. This means that parties must be given an opportunity to respond to a preliminary view or adverse evidence gathered during the investigation if it is relevant to the decision making about that matter. Parties who are affected adversely may include the following:

- the complainant;

- any other individual whose personal information was involved, Officers involved in handling the personal information subject to the complaint or breach; and

- any Officers responsible for the business unit where the incident occurred.

If an affected party makes a submission in response to the preliminary view of the Investigating Officer or adverse evidence, the Investigating Officer must consider that submission before making a decision on the matter.

Any comments made by a party in this instance may form part of the final complaint report or response to the complaint.

15. Outcome of a Privacy Complaint

Where a privacy complaint is substantiated, the Investigating Officer must have regard to the complainant's suggestion for resolution.

Remedies which may be available to the complainant include:

- a written or verbal apology;
- if appropriate, an explanation as to how or why the breach occurred;
- organisational change such as changes to policies, procedures or operational practices;
- privacy training or TFN handling training for the relevant officers and business unit; and
- a report will be prepared outlining the complaint, its assessment and investigation and its recommended resolution. The report will include all relevant dates to demonstrate the requisite timeframes have been met.

16. Response to a Privacy Complaint

The Approving Officer will consider the privacy complaint and decide on the most appropriate remedy, having regard to the relevant and reliable evidence and affected parties' submissions. As outlined in the example letters below, any response to the complainant must include:

- the outcome of the investigation;
- the decision of the relevant Officer, including whether the complaint was substantiated or not;
- a clear explanation of how the decision was made and the information relied upon to make that decision;
- information about any changes implemented as a result of the complaint;
- where the matter relates to a TFN or TFN information and is a serious data breach, provide guidance to the complainant on the steps they may take to limit the harm arising out of the breach;
- any resolution to the complaint if substantiated, as outlined at paragraph 15; and
- information about the complainant's right under section 166(c) of the IP Act to make a complaint to the OIC if they consider DJAG's response to their complaint not to be an adequate response.

Examples of closure letters (unsubstantiated and substantiated findings) which can be sent to the complainant at the conclusion of an investigation can be found at Complaint Response (PRV110); Complaint Response/Referral to ESU letter (PRV060).

17. Finalising the Complaint File

Before finalising the complaint file, ensure that all information has been accurately and correctly documented both in CMS and eDocs and any evidence stored or returned.

18. Consider any Systemic Issues raised by the Complaint and Possible Responses

There may be circumstances where an investigation into a privacy breach indicates that the breach occurred because a procedure, policy or business practice was insufficient to protect and manage personal information in line with the IPPs; insufficient secure storage of personal information; lack of privacy training to staff; or an information technology security breach.

Where an investigation indicates that a privacy breach has occurred, the Investigating Officer may recommend that the business unit review and update its business practices and include any of the following:

- Privacy training to the relevant individual and/or work unit.
- TFN handling training.
- Amendment of policies, forms and/or collection notices to ensure clear guidance and compliance with the IPPs.
- Providing additional accessible information to ensure privacy concepts are understood.
- Improve security and storage measures in accordance with IPP 4.
- Steps to improve data accuracy in accordance with IPP 4 and IS18 Information Security Policy (IS18:2018).

19. Definitions

Term	Definition/Explanation
Approval Table	Contains information about the receipt, assessment and approval of a triage assessment undertaken in relation to a privacy complaint or privacy breach.
Action and Classification Table	A table containing information about the different types of privacy breaches and issues raised in privacy complaints, and the risks/harm to DJAG, stakeholders, complainant, and other individuals as a result of these issues. The table identifies the level of investigation required and whether referral to ESU or Executive Management is required.
Serious data breach	A data breach that is likely to result in serious harm to an individual from the perspective of a reasonable person in DJAG's position. Serious harm includes serious physical, psychological, emotional, financial or reputational harm (refer to OAIC website).
Tax File Number (TFN)	A TFN is a TFN as defined in Part VA of the Commonwealth *Income Tax Assessment Act 1936.*
Tax File Number Information (TFN Information)	Information, whether compiled lawfully or unlawfully, and whether recorded in a material form or not, that records the TFN of a person in a manner connecting it with the person's identity.