Department of Justice and Attorney-General

Privacy Handbook

2021

Queensland Government

Document information

Security Classification	Unclassified
Date of review of security classification	1 December 2020
Authority	Director-General, Department of Justice and Attorney-General
Documentation status	Final release
Next review date	December 2023
Document reference	eDocs No. 5442586

Version history

Version	Notes	Changed by and date
0.1	Original document created in October 2020	October 2020
0.2	Amendments by Director incorporated	October 2020
0.3	Consultation draft incorporating comments from business units	November 2020
1	Final document	December 2020

Document owner/enquiries

All enquiries regarding this document should be directed in the first instance to Right to Information and Privacy, Department of Justice and Attorney-General (DJAG, the Department).

This document is owned by the Director, Right to Information and Privacy, DJAG, who is responsible for the development and ongoing review of the policy.

Document approval and review

This document was approved by the Acting Director-General, DJAG on 14 January 2021. This policy is reviewed every three years or as necessary in response to legislative change. The next scheduled review is December 2023.

Security classification

This document has a security classification of UNCLASSIFIED.

License

Contents

Purpose

This handbook is designed to give you a general overview of when you might need to consider the obligations in the *Information Privacy Act 2009* (IP Act) and what to do, where to look for more information or who to ask for advice when you need it.

This handbook also references resources and toolkits that are available and ready for you to use on the Department's intranet page.

The Department has diverse functions and our roles and interactions with personal information will always vary depending on what we do for work. This guide won't cover all those circumstances so, if:

1. you're sure that you're dealing with personal information; and
2. you've looked at this guide and the material referenced by it; and
3. you're still not sure how to comply with the IP Act in your circumstances, you should contact privacy by phone on (07) 3738 9893 or by email at: privacy@justice.qld.gov.au.

The information in this guide is not intended as legal advice. All business units should seek and be guided by their own legal advice if there is any doubt about the practical application of the IP Act.

What is privacy?

When we refer to information privacy, we're not necessarily referring to secrecy or confidentiality. We are referring to the responsible handling and management of personal information in the hands of Queensland Government agencies like ours. There is a lot of personal information available to us that is not necessarily confidential. However, the personal information we manage and handle as part of our work still attracts legal obligations under the IP Act.

It is also important to note that some personal information may also be confidential under legislation. The confidentiality provisions in your enabling legislation will impact on the operation of the IP Act because the IP Act is intended to operate subject to provisions in other Acts relating to the collection, storage, handling, access, amendment, management transfer, use and disclosure of personal information.

The key message here is that you should also have a good knowledge of the information management and handling provisions in the enabling legislation under which you do your day to day work as well as a good knowledge of the Department's obligations under the IP Act.

If you don't know the enabling legislation you work under, you should ask your supervisor or manager.

What does privacy have to do with me?

Every Queensland Government department, all local councils, public hospital and health services and other public authorities have obligations under the IP Act. Section 27 of the IP Act requires us all to comply with our privacy obligations.

We collect, use, store and disclose personal information every day so we can do our jobs. However, we manage and handle personal information so regularly that sometimes we don't stop to think about what our obligations are in relation to it.

It's important to remember that the purpose of the IP Act is not to stop the handling of personal information or prevent its disclosure. It is to set a framework for the responsible and ethical handling of personal information given to us so we can provide services to the community.

In summary, the IP Act affords our clients and customers the same privacy protections that we would expect from our local councils or Queensland Government departments we interact with as citizens and individuals.

What is personal information?

Personal information is a defined term under the IP Act as:

"…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."

We can see from the definition that 'personal information' is a broad concept. In summary, it means that if a person can reasonably be identified from general information, the general information is personal information. The information can be in writing or not, true or not, or on a database or not.

If it's easy enough to ascertain someone's identity from information; the information is personal information for the purposes of the IP Act.

> *Example[1]:*
>
> *Jodie and Mary work together in an Office of Liquor and Gaming Regulation Regional Office and they are talking about a person in the lunchroom. Jodie is talking to Mary about a troublesome liquor licensee who owns and operates a licensed venue in the same small town Jodie and Mary's Regional Office is located. This liquor licensee is also a frequent contact who is having a dispute with OLGR about an amendment to his liquor licence.*
>
> *During the conversation, David, who works in the same building as Jodie and Mary but for the Department of Transport and Main Roads, and who lives in the local area, walks into the lunchroom and says, "Oh, that's Robert you're talking about! He's my neighbour. What was it you said about him being a pain about his license?"*

Without meaning to do so, Jodie has passed Robert's personal information on to David. Unless David was authorised to know that his neighbour was making an application for an amendment to his liquor licence, this might be a breach of the disclosure principle in the IP Act.

It's important to note that 'individual' is not defined in the IP Act, but it is defined in the *Acts Interpretation Act 1954* as a *'natural person'*. This means that only living people can have personal information. Despite this, the IP Act allows for the amendment of a deceased person's personal information by a person permitted to do so under the IP Act, for example, their next of kin.

Information about a deceased person is no longer personal information in relation to the deceased person, but it may still be the personal information of living individuals. For example, coronial records often contain personal information about the deceased person's family and friends and health records may contain biological information about the family, such as inheritable medical conditions.

[1] All names in the examples provided in this document are made up for the purposes of these examples. Any identification to an individual is purely coincidental.

Privacy Impact Assessments

If you are doing any work which involves the:

- collection or intake of personal information;
- use of personal information to perform work functions;
- storage of personal information in a new way, especially cloud-based storage hosted overseas;
- transfer of personal information from one part of the agency to another;
- disclosure of personal information to an entity outside of the Department; and/or
- contracting with service providers who will handle personal information on our behalf,

then you are involved in handling personal information and you will need to make sure you are complying with the Department's privacy obligations and any information management obligations you have in your enabling legislation.

If you are considering the implementation of a new business process or system that relates to one of the items listed above, or if you are considering a significant upgrade to an existing legacy system containing personal information, the Department's Right to Information (RTI) and Privacy recommend undertaking a Privacy Impact Assessment (PIA) Threshold Scan in relation to your project or activity prior to its implementation or roll-out. The Threshold Scan will identify whether a full PIA is required for the new process. PIAs are assessments which identify, report on and recommend mitigation strategies for key risks to compliance with our obligations under the IP Act. PIAs or obtaining advice on key privacy non-compliance risks of a project or activity is an essential part of the work leading up to the approval and implementation of your project or activity.

For more information and guidance on how to conduct a PIA refer to the Office of the Information Commissioner's web page or, contact privacy@justice.qld.gov.au.

Collecting personal information

We collect personal information to transact business, give effect to policies, engage in law enforcement or investigation activities, pay our staff, contact our clients and applicants and for many other reasons related to doing our work for Queensland Government.

In summary, we collect personal information so we can do our jobs effectively and keep in touch with the people who transact with our Department.

Our collection obligations are set out in Information Privacy Principles (IPPs) 1, 2 and 3 in Schedule 3 to the IP Act. These principles limit the collection of personal information to information we need for a for a lawful purpose directly related to the Department's functions or activities.

Collecting personal information for an undefined future purpose on the basis that the information may be useful at some point in the future may exceed this limitation. This makes it especially important to consider whether, at the time you are collecting the personal information, you really need all of the personal information you propose to collect in order to undertake your task.

The principles also require that we collect personal information in a fair and non-intrusive way, including letting people know why we are collecting personal information (IPP 2), whether we have any statutory requirement or authorisation to collect the information (and if so, what it is) and who we may give the information to. We often let people know by giving them a privacy collection statement. You can generate your own IPP 2 draft privacy statement using the Privacy Statement Generator.

Remember that our obligation to make people generally aware of the matters listed in IPP 2 doesn't prescribe how we make people generally aware of those matters (this can happen verbally, in writing or even by using signage).

That said, for evidentiary purposes and where possible, compliance with IPP 2 in writing is preferred. If you are unable to give an IPP 2 privacy statement to an individual in writing, it's good practice to make a file note of your conversation.[2]

If we make people generally aware of the matters listed in IPP 2 before, or as soon as practical after, the collection of the personal information then we comply with the requirements of IPP 2.

When we first collect personal information, we also have an obligation (IPP 3) to take reasonable steps to check the quality of the personal information we receive. Good quality personal information helps us to make good decisions based on complete, current and accurate personal information. This is especially important because some of the decisions we make will impact directly on the rights and obligations of members of the community who interact with us.

> *Example:*
>
> *Joan is a customer of "Anthea's Curls Hairdressing and Beauty". Recently, Joan was injured in a serious bleaching incident which made a lot of Joan's hair fall out and which resulted in her remaining hair turning a vibrant blue. Joan is a solicitor and as a result of the incident, she took substantial time away from her work. Joan approached Anthea's Curls for a refund and some kind of compensation and Anthea's Curls refused on the basis that they'd already spent the money on the bleaching products and had already paid the hairdresser for the time spent on Joan's new hair style.*
>
> *Consequently, Joan made a complaint to the Office of Fair Trading (OFT). Soon afterwards, Joan saw some nasty comments on her social media page made by Anthea's Curls about how Joan is a whinger who tries to obtain free products and services by complaining to government agencies.*
>
> *Joan immediately contacted OFT and demanded to know how Anthea's Curls became aware of her complaint. The OFT officer let Joan know that it is clear in the complaints manual of OFT which is published online, that the substance of complaints are normally disclosed to a trader so they may respond to the complaint in accordance with the principles of procedural fairness.*
>
> *Joan said she was never made aware of the existence of the manual and made a complaint to RTI and Privacy about the unauthorised disclosure of her personal information – namely – that the fact she'd made a complaint against Anthea's Curls was revealed to Anthea's Curls.*
>
> *RTI and Privacy investigated the complaint and found that while the disclosure was lawful, OFT did not take reasonable steps to give Joan proper notice that her information would be disclosed to Anthea's Curls as part of OFT's investigation.*

We can use, disclose, and store personal information if we tell people up front that we will collect, use and disclose their personal information and why. Letting people know why we're collecting their personal information and what we're going to do with it is not only compliant with the collection requirement in IPP 2, it is a practical example of how fair collection works day-to-day.

[2] For evidentiary purposes, it is also a good idea to write your file note at the time of or immediately after your conversation (i.e. a contemporaneous file note).

By not complying with its obligation to make Joan generally aware of the matters listed in IPP 2, OFT was not being fair to Joan when it collected Joan's personal information in her complaint. If Joan knew that her personal information was likely to be disclosed to Anthea's Curls it would not have come as a surprise to Joan and OFT may have avoided the privacy complaint altogether.

What OFT should have done in this case was to give Joan a compliant privacy notice on the letter acknowledging her complaint which would have given Joan notice of the minimum required matters as soon as practicable after she disclosed her personal information to OFT.

Even if Joan still decided to complain, OFT could have relied on the disclosure exception in IPP 11 which allows disclosure where we have fulfilled our obligation to tell people up front that their personal information would be disclosed to relevant parties.

Note that IPP 2 only applies in circumstances where we collect personal information from the person the personal information is about.

Here is what to consider when you're collecting personal information from the person to whom the personal information relates:

1. think about how much personal information you absolutely need to undertake your task and only collect that much of it that is relevant to the work you need to do;
2. once you've decided on the personal information you're going to collect, check to see whether any legislation you administer for your work authorises or requires the collection (don't worry if there is no legislative provision, you can still collect the information);
3. think about how you are going to use the personal information (e.g. will you consider it as part of an application process, will you add it to a mailing list etc);
4. think about who you will usually give the information to (e.g. Queensland Health, Queensland Police Service, Queensland Fire and Emergency Services etc);
5. outline the above information in a compliant IPP 2 privacy statement. Generate a draft IPP 2 privacy statement using the Privacy Statement Generator and have it checked by RTI and Privacy;
6. if you think that the information you are collecting is incomplete, out of date, inaccurate or misleading, take reasonable steps to improve the currency, accuracy and completeness of the personal information.

If you would like to read further information on privacy and complaints management, see Privacy in Complaints Management – Disclosure and Natural Justice and Privacy in Complaints Management - Anonymity and Confidentiality. You can also see the Department's Privacy Complaints and Breaches Policy and Procedure on the Department's Intranet site.

Storing and securing personal information

Information security plays an important role in the responsible handling of personal information in our workplace. Usually, if personal information is secured in accordance with our Information Security Policy, personal information will not end up in the wrong hands.

IPP 4 is the storage and security principle which requires Queensland Government agencies to do what is reasonably necessary to store and secure personal information in a way consistent with the high expectations the community has of us in relation to how we manage their personal information.

IPP 4 imposes a strict, positive obligation on the Department to implement technical and physical security controls that reflect the sensitivity of the personal information we are storing.

It provides that we must store and secure personal information in a way that will ensure that it is protected against:

- loss; and
- unauthorised access, use, modification or disclosure.

Where it is necessary for the information to be given to a person in connection with a service to the Department, IPP 4 also requires that the Department takes all reasonable steps to prevent unauthorised use and disclosure by the person the Department gives the information to.

The protections listed above must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided. The more sensitive or the more harm or damage that could arise out of a security breach, the stronger the physical and technical controls over the information need to be.

Determining the sensitivity of the personal information we collect may mean undertaking an information security classification exercise. For Queensland Government, the classification of the personal information will determine the technical security controls required for the classification.

The Department has useful resources on the intranet that can assist you with this process:

Information Security Policy

Information Access and Use Policy

Information Security Risk Appetite Statement

Information Security Classification Tool

Queensland Government Information Security Classification Framework

In addition to the technical security controls we must consider, we must also consider what physical and procedural controls we can implement to secure personal information. These actions can range from ensuring that personal information is not left on shared printers; if we are using a whiteboard, ensuring that personal information is not left on the board when we've finished using it; securing floors and physical record storage areas; protecting documents including while travelling with them; and being aware of our surroundings when we are discussing personal matters in public or shared spaces.

> *Example:*
>
> *The Department has brought in a new database to manage incoming applications for victim assistance. Briony is the local expert on how the database operates, so Briony oversees training her other colleagues on how to use the database. Andy is a graduate and new to the Department. Andy notices that the information in the database contains real personal information. When Briony steps away to answer a call, Andy runs a search on an old friend of his and discovers that his old friend's personal information is in the database. The next time Andy sees his old friend, Andy tells his friend about all the information about his friend on the database, including another officer's opinion that Andy is a little eccentric.*

The IP Act isn't designed to stop us from training our staff about our databases, systems and procedures. However, using sample data instead of the personal information of real applicants, to train our colleagues in the use of new systems and databases would have mitigated the risk of Andy using the system to gain unauthorised access to his old friend's information.

Andy's actions, if they can be shown to be wilful, may also be a breach of the *Code of Conduct for the Queensland Public Service* and may be an action that is referred to the Crime and Corruption Commission or even amount to a computer hacking crime under the *Criminal Code.* While the obligations in the IP Act are on Government agencies, wilful actions or omissions in relation to Government information that do not comply with our obligations as public servants are matters that People and Engagement and the Ethical Standards unit can become involved in.

It's also important to note that the obligation in IPP 4 is about systems and processes rather than human error or unforeseeable events. This means that while personal information may be lost or exposed to unauthorised disclosure due to unforeseen circumstances such as a disaster event or unforeseeable intrusion into our systems and databases, these will not breach the strict requirements in IPP 4 unless it can be shown that all reasonable controls were not in place to prevent or mitigate the harm arising out of these events.

If you are proposing to store personal information on a cloud server that is based overseas, see the section below on 'Transferring personal information outside Australia'.

Here are some things to consider in the context of securing personal information.

1. Is the personal information subject to some other protections such as a confidentiality provision in an Act? If so, the personal information must be managed consistently with that provision or confidentiality agreement in so far as the provision or agreement covers what you can and cannot do with the information.
2. Has the information been classified in accordance with the Department's security classification process? An information security classification will give you an indication of what the minimum security requirements are for the personal information.
3. Does the way you are proposing to store and secure the personal information comply with the minimum security requirements for the information?
4. Can you avoid the use of shared printers, fax machines, tablets and smart devices?
5. Have you encrypted the USB stick you are using?
6. Are the access authorisations for the type of personal information you are storing adequate?
7. Are physical security measures appropriate in the circumstances? For example, secured floors, compactuses and private interview rooms?
8. If the information is being stored in a database, will access to the database be restricted by role?
9. Will there be any regular access privilege audits to keep track of who has access to the information and when?
10. Is there any back up or disaster-recovery plan in place for the information?
11. Is the information going to be stored overseas? If yes, see 'Transferring Personal Information outside of Australia'.

Letting the community know the types of personal information we hold

IPP 5 requires the Department to take all reasonable steps to ensure that a person can find out:

- Whether the Department has control of any documents containing personal information; and
- The type of personal information contained in the documents; and
- The main purposes for which personal information included in the documents is used; and
- What an individual should do to obtain access to a document containing personal information about the individual.

Our Department complies with this obligation on its corporate web page.

Accessing and amending personal information

IPPs 6-7 of the IP Act give people a right to access and amend personal information held about them by Queensland Government. This means you can apply to any Queensland Government agency to view or obtain a copy of the personal information these entities hold about you in the same way that our clients and customers can apply to us for their personal information.

Giving individuals the right to access and amend their personal information includes giving them a right to apply to do so without charging them an application fee.

In addition to the right to see or obtain a copy of the personal information Queensland Government agencies hold, individuals also have a right to apply to amend their own personal information if they consider it is incorrect, out of date or misleading. These rights are in Chapter 3 of the IP Act. Giving an individual the right to take action to keep their personal information complete, current and correct is another way of ensuring the good quality of the personal information in our Department's possession and control.

It's important to note that the access and amendment provisions in the IP Act are not intended to overturn Government decision-making processes that were validly made on the basis of personal information that was current, complete and correct at the time the relevant decision was made.

However, if the Department does not agree to a request for personal information to be amended in the way the individual has requested, the Department may place a notation on the file or database on which the personal information is held with the individual's version of what the individual considers to be their complete, current and correct personal information.

For more information on accessing and amending personal information, see RTI and Privacy's "Access and Amendment" on Right to Information and Privacy's intranet page and the Office of the Information Commissioner's (OIC) website.

The difference between 'use' and 'disclosure' of personal information

Before moving onto the next part of the life cycle of personal information in the Department's possession and control, it's timely to have a look at the difference between 'using' personal information and 'disclosing' personal information. These two related but different acts or practices in relation to personal information are defined in section 23 of the IP Act.

In summary, *using* personal information can be action other than the action of disclosing the information. Using personal information are acts or practices like:

- Accessing personal information held on our databases or shared drives;
- Moving personal information from one part of the Department having one type of function to another part of the Department having another function; or
- Taking personal information into consideration as part of a decision-making process.

Disclosing personal information is when the following three conditions are met:

1. An entity (the *first entity*) *discloses* personal information to another entity (the *second entity*) if –
   (a) the second entity does not know the personal information, and is not in a position to be able to find it out; and
   (b) the first entity gives the second entity the personal information, or places it in a position to be able to find it out; and
   (c) the first entity ceases to have control over the second entity in relation to who will know the personal information in the future.

If all (a)-(c) apply to the circumstances, then it is likely that the act or practice in relation to the personal information is a disclosure and not a use.

Checking for accuracy, completeness and currency of personal information

In addition to the data quality provisions contained in IPPs 3 and 7, IPP 8 requires us to check the quality of personal information before we use it. This means we have at least two opportunities to check the quality of the personal information we have obtained – the first when we collect the personal information, and the second before we use the personal information (as defined by section 23 of the IP Act).

IPP 8 requires us to take reasonable steps, having regard to the purpose for which the information is proposed to be used, to ensure that the personal information we use to deliver services, contact our customers and clients and make Government decisions is accurate, complete and up to date.

> *Example:*
>
> *Mike is the President of a not-for-profit organisation delivering gambling counselling to youth in rural Queensland. Mike applied to the Office of Liquor and Gaming Regulation for grant funding from the Gambling Community Benefit Fund. Mike provided his personal information on the grant application form. David received the completed form for processing and started work on Mike's application. Before responding to Mike, David emailed his supervisor to check the draft letter. David's supervisor has the same first name as one of David's golfing partners and unbeknownst to David, the auto-complete feature on Microsoft Outlook populated the "to" field in the email with the golfing partner's email address and David inadvertently emailed the draft letter to his golfing partner instead of his supervisor.*
>
> *Because David did not check the accuracy of his supervisor's email address before using the email address, this may amount to an unlawful or unauthorised disclosure of personal information to an external person.*

Limits on using personal information

As stated earlier in this handbook, the purpose of the IP Act is not to limit the legitimate flow of personal information for the purpose of undertaking our workplace tasks and activities.

However, IPP 10 generally limits the use of personal information to the purpose for which the Department originally obtained the information. This means we must decide *before* we collect personal information, on how we will use the personal information.

In fact, if there is no identifiable lawful and relevant work-related purpose identified for obtaining personal information, this may raise concerns about whether we should have obtained the information in the first place.

In order to facilitate the responsible flow of personal information throughout the Department, IPP 10 provides exceptions to the general limitation.

In summary, you can use personal information for a purpose that is not related to the purpose for which the information was first obtained in the following circumstances:

- if the individual the personal information is about agrees to the other use;
- if the Department is satisfied on reasonable grounds that the other use is necessary to lessen or prevent as serious threat to the life, health, safety or welfare of an individual or the public;
- if the Department is satisfied on reasonable grounds that the use of the information for the other purpose is necessary for certain actions for or by a law enforcement agency (see below);
- if the other use is directly related to the original use;
- where the use is required for research in the public interest and it's not practical to obtain the agreement to the use for the research purpose and the use doesn't involve the publication of personal information.

Example:

Phaedra works in the Department as an Advisor. Trevor, Phaedra's Director, would like to nominate Phaedra for an Excellence Award for Customer Focus. In order to nominate Phaedra, Trevor must use some of Phaedra's personal information, including her personal email address. Trevor has access to this information, which is contained in Phaedra's commencement documentation.

Trevor accesses Phaedra's personal information on Phaedra's commencement paperwork and sends an email to Phaedra's work email address saying that he would like to nominate Phaedra for an Excellence Award for Customer Focus and asking for Phaedra's permission to use her personal email address for this purpose. Phaedra agrees, and the 'other' use of the personal information is allowed because of the 'agreement exception' in IPP 10.

Need help deciding whether to use personal information for a purpose other than the purpose the Department obtained it? Contact RTI and Privacy at privacy@justice.qld.gov.au.

Limits on disclosing personal information

IPP 11 limits the disclosure of personal information to the person whom the personal information relates to unless circumstances, similar to those excepting the general limitation on the use of personal information, apply. While the circumstances excepting the general limitation on the use of personal information are substantially the same as those excepting the limitation on the disclosure of personal information, there is one important difference. This is the exception in IPP 11(1)(a).

IPP 11(1)(a) refers us to IPP 2. IPP 2, the second collection principle, is the principle that requires the Department to inform individuals:

1. why (the purpose for which) we are collecting the personal information; and
2. whether the collection is authorised or required by a law, and if so, the name of the law; and
3. who we would usually give the personal information to; and
4. if we know, who the entity we give the personal information to would usually give the information to.

If we have made the individual generally aware of the above matters as required by IPP 2, then we can disclose the personal information to the entity or entities we originally referred to in the IPP 2 statement or signage.

Complying with our collection obligations from the outset (when we first receive the personal information) supports the future lawful disclosure of personal information.

A common enquiry is whether we can give people certain personal information without breaching the IP Act. Consider this scenario:

> *The Justices of the Peace Branch of the Department regularly deals with complaints from members of the public about the conduct of qualified Justices of the Peace and Commissioners for Declarations. Leanne is very unhappy with the service she received from a Justice of the Peace she saw at her local shopping centre in Woodridge. Leanne is unaware that her complaint is one of a series of complaints received about the same Justice of the Peace over the last three months. Consequently, the Justices of the Peace Branch decide to investigate the allegations made by all the complainants.*
>
> *Jennifer, who works in the Justices of the Peace Branch, is considering letting Leanne and the other complainants know about the investigation and the fact that the investigation is taking place because of a number of complaints made against the same Justice of the Peace within a short period. Jennifer is thinking of disclosing this information, so the complainants know the Department treats complaints seriously.*

Jennifer knows that information relating to the number of complaints made against the Justice of the Peace is the personal information of the Justice of the Peace and knows she should only disclose that information to the Justice of the Peace.

Given there is no requirement to let complainants know this information in any legislation or under any common law principles, Jennifer goes to IPP 11 in the IP Act and confirms that none of the exceptions in IPP 11 would apply to the proposed disclosure of the personal information to the complainants.

As a result, Jennifer does not disclose to any of the complainants that the Justice of the Peace was subject to several complaints.

Transferring personal information outside Australia

Section 33 of the IP Act generally prohibits the transfer of personal information outside of Australia unless one or more of the exceptions listed under section 33 apply to the circumstances of the transfer.

We may transfer personal information overseas more often than we think. For instance, the information held in every Google, Live and Yahoo email account is stored in the United States of America. So, too is any data generated and stored by Survey Monkey, Salesforce.com and countless other multinational organisations whose services we may use daily.

With increasing numbers of business areas storing or contracting for the storage and management of information on the cloud, this provision becomes increasingly relevant to our daily work practices.

The rationale behind this provision was for personal information to be protected in the same or in a substantially similar way as it is protected in Australia, if the personal information is transferred overseas.

It's important to know that 'transferring' personal information is not the same as sending personal information through an overseas jurisdiction. For section 33 to apply to the circumstances of the transfer, the personal information must 'rest' in the overseas jurisdiction.

The prohibition against transferring personal information overseas is not absolute and can be overcome if any one of the following exceptions apply to the circumstances:

- the individual to whom the personal information relates agrees to the overseas transfer;
- the transfer is authorised or required under a law;
- the Department is satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual or the public;

  OR

  Two or more of the following applies:

- the Department reasonably believes that the overseas entity receiving the information is subject to a law, binding scheme or contract that effectively upholds the same or substantially similar principles for the fair handling of personal information as the IPPs; and/or
- the transfer is necessary for the purpose of the Department's functions in relation to the individual; and/or
- the transfer is for the benefit of the individual and it isn't practical for the Department to seek the agreement of the individual, however, if the Department could ask, it would be more likely than not that the individual would give their agreement; and/or
- the Department has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs.

If you are in doubt about whether any of the exceptions apply to your circumstances, email privacy@justice.qld.gov.au for advice.

Giving personal information to contracted service providers

The Department often enters into agreements or engages contracted service providers in order to help it deliver new projects and help it improve existing projects and programmes. Often, the work we engage others to do on our behalf involves the transfer of personal information to service providers or requires the collection of personal information by service providers on behalf of the Department.

Where personal information is given to, or collected by, service providers to deliver services to us or on our behalf, the Department must consider the effect of sections 34-37 of the IP Act. In summary, these provisions require us to bind contracted service providers to the relevant parts of the IP Act as if they were the Department.

Where a service provider is appropriately bound (often by way of deed or contract) to the relevant parts of the IP Act, the obligations in the IP Act that would otherwise apply to the Department will apply to the service provider.

This means that if there is a data breach in the hands of the service provider or an act or practice of the service provider contravenes any of the obligations of the IP Act, it is the service provider rather than the Department that is responsible for the contravention.

If you are involved with the development of a software solution, it is likely that you will need to follow the Queensland Information Technology Contracting Framework (QITC).

Each contract in the QITC Framework has standard terms and conditions that will normally adequately bind contracted service providers to the IP Act, or, if appropriate, to the Commonwealth *Privacy Act 1988*.

Alternatively, you may engage a contractor under a Standing Offer Arrangement (SOA). If you are, check to see that the heads of agreement under which the SOA is made includes the standard privacy clause (see clause 19 of the Standing Offer Arrangement Conditions).

Before entering into any agreement with service providers, you should ensure that you have authorisation to do so and that you seek and be guided by legal advice on the most appropriate way to bind contracted service providers to the relevant parts of the IP Act.

Appropriately binding service providers in the way provided for by sections 34-37 of the IP Act will also:

- help the Department comply with its obligation in IPP 4(1)(b) to take all reasonable steps to prevent unauthorised use or disclosure of personal information by the contracted service provider; and
- constitute one of the two exceptions under section 33(d) (transfer of personal information outside of Australia).

If you are considering entering into an agreement with an organisation by accepting the organisation's terms and conditions rather than binding the organisation to the Department's terms and conditions, please consider the information in 'Guidelines for supplier terms and conditions – ICT products and services'.

Law enforcement entities, law enforcement functions and personal information

The IP Act makes a number of exceptions for circumstances where personal information must be collected, accessed, used or disclosed for 'law enforcement purposes' by 'law enforcement agencies'. None of these exceptions operate as a rule and are always subject to an assessment having regard to the circumstances of each case.

A law enforcement agency is defined by the IP Act in its Dictionary at Schedule 5. The definition of a law enforcement agency in Schedule 5 for the purposes of section 11(1)(e) of the IP Act is *"an enforcement body within the meaning of the Privacy Act 1988 (Cwth)"* or otherwise:

- The Queensland Police Service;
- The Crime and Corruption Commission;
- Queensland Corrective Services; and
- DJAG to the extent that it has responsibilities for:
  - The performance of functions or activities directed to the prevention, detection, investigation, prosecution or punishment of offences and other breaches of laws for which penalties or sanctions may be imposed; or
  - The management of property seized or restrained under a law relating to the confiscation of the proceeds of crime; or

- The execution or implementation of an order or decision made by a court or tribunal.

If you are approached for personal information by a law enforcement agency without a warrant or a subpoena, you will need to be sure that:

- the requesting officer has been authorised by their commanding/authorised senior officer to request the information;
- the requesting officer has detailed the purpose for which the personal information is required (e.g. investigation of an alleged offence under the *Criminal Code Act 1899*);
- you communicate to the requesting officer that the disclosure is being made pursuant to the law enforcement exception in IPP 11 and that the use of the personal information is to be restricted to the stated law enforcement purpose; and
- you keep a record of the personal information you released on the file (whether paper or electronic) from which the information came.

Reasonable grounds for non-compliance – law enforcement

Over and above the exceptions in IPP 10 and 11 for law enforcement agencies or agencies with law enforcement functions, section 29(1)(d) of the IP Act allows law enforcement agencies to consider, on a case by case basis whether noncompliance with certain IPPs is necessary in the circumstances. If it is decided on reasonable grounds that non-compliance is necessary with:

- IPP 2;
- IPP 3;
- IPP 9;
- IPP 10; or
- IPP 11

a record of that decision should be kept including the rationale for the decision and the IPPs the Department has considered necessary not to comply with in that case. This will support any further enquiries in relation to the considered decision not to comply with the above IPPs.

If you have any doubts about whether you may be exempt from the above IPPs, please seek guidance from RTI and Privacy by email at privacy@justice.qld.gov.au.

Complaints and breaches

The IP Act contains a complaint management framework.

It is important to act quickly in relation to privacy breaches and complaints. If a breach of any of the provisions of the IP Act is identified early, more effective measures can be taken to contain the further dissemination of the personal information. For more information contact RTI and Privacy as soon as possible after you become aware of the matter at privacy@justice.qld.gov.au or (07) 3738 9893.

If a complaint is received, and it meets the requirements of the IP Act, the Department has 45 business days to investigate the complaint, collect and assess the evidence, make recommendations for any changes to business processes to mitigate the risk of future breaches and complaints and respond to the complainant before the complainant has standing to make a privacy complaint to the Office of the Information Commissioner.

This means you must refer any complaint which covers the management and handling of a person's personal information directly to RTI and Privacy as soon as possible after you receive it. We will advise you on the next steps when we receive your notification.

Client complaints (including privacy complaints) are managed under the DJAG *Client Complaints Management Framework.* Under the Framework, you must record and report the privacy complaint using the client complaints register, even though RTI and Privacy will be advising you and assisting in the Department's response to the privacy complaint. For more information on client complaints management go to: https://intranet.justice.govnet.qld.gov.au/divisions-and-branches/corporate-services/corporate-governance/complaints-management.

If a person requests information about making a privacy complaint or if there is any doubt that a complaint is a privacy complaint, please contact RTI and Privacy by email at privacy@justice.qld.gov.au or by telephone (07) 3738 9893. For more information on how the Department deals with privacy complaints, see the Information Privacy Complaint and Investigation Policy and Procedure.

Privacy and Human Rights

The *Human Rights Act 2019* commenced in its entirety on 1 January 2020 and forms part of the administrative law obligations and oversight mechanisms that hold government to account. The Human Rights Act protects fundamental human rights drawn from international human rights law, including the right to privacy and reputation. To learn more on privacy and reputation as a human right go to: https://www.qld.gov.au/law/your-rights/human-rights.