Obligations of contracted service providers: *Information Privacy Act 2009*

Background

The Department of Children, Youth Justice and Multicultural Affairs (the department) engages contracted service providers (CSPs) to perform some of its functions. CSPs often handle personal information in the course of performing those functions.

The standard terms of Queensland Government contracts bind CSPs to comply with the *Information Privacy Act 2009* (IP Act) in relation to personal information.

Note: Some CSPs may have other privacy obligations (e.g. under the federal *Privacy Act 1988*). However, where they are performing obligations under a State contract, the terms of the contract and the Queensland IP Act will apply (sections 3 and 7B, Privacy Act), instead of the federal Privacy Act.

Information privacy is also covered by the Human Services Quality Framework for CSPs providing human services (standard 1.7).

Policy and practice

CSPs must have a privacy plan or policy that outlines how they protect the privacy of people whose personal information they collect, use and disclose.

The Office of the Australian Information Commissioner has guidelines about developing a privacy policy available at Chapter 1: APP 1 — Open and transparent management of personal information — OAIC[1]

CSPs must provide privacy training and reminders to staff, to ensure that all staff understand their privacy obligations.

CSPs may also find it useful to nominate a staff member to be a Privacy Contact Officer, to provide privacy guidance and advice to other staff and deal with privacy issues.

If a bound CSP fails to comply with its privacy obligations, it will be liable for any breaches under the IP Act (including potential liability to pay compensation of up to $100,000 per breach)[2] and possibly breach of contract.

Given the liability that they may incur if they fail to comply with their obligations under the IP Act, it is recommended that bound CSPs seek independent legal advice as necessary, about how to meet their privacy obligations.

'Personal information'

The IP Act governs collection, management, use and disclosure of *personal information*.

'Personal information' is defined 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.*[3]

An *individual* is a natural person and does not include a company or corporation. Information may reveal a person's identity even if their name is not mentioned, if their identity can be deduced.

[1] Although the contract requires CSPs to comply with the Queensland *Information Privacy Act 2009*, CSPs can rely on a Privacy plan or policy developed in accordance with the *Privacy Act 1988* (Cth).

[2] *Information Privacy Act 2009,* sections 34-37

[3] *Information Privacy Act 2009,* section 12

CSP staff must be able to identify personal information and how it should be managed.

Obligations under the IP Act

The IP Act requires a bound CSP to comply with the 11 Information Privacy Principles (IPPs) set out in schedule 3 of the Act and summarised at the end of this fact sheet.[4]

Bound CSPs are also required to comply with section 33 of the IP Act, which prohibits the transfer of personal information outside Australia, except in limited circumstances.

Overseas transfer happens if the CSP uses a cloud-based service which is hosted overseas, or if personal information is posted on the internet and accessed from overseas.

The standard contract terms require that CSPs seek consent from the department if they intend to send personal information overseas. CSPs must provide evidence of how they will meet their privacy obligations if personal information is transferred overseas.

The Queensland Office of the Information Commissioner (OIC) has published guidance about when personal information may be transferred overseas Sending personal information out of Australia | Office of the Information Commissioner Queensland (oic.qld.gov.au)

Obligations under other legislation

The IP Act is subject to other legislation that may restrict the disclosure of information, e.g. confidentiality provisions in *Child Protection Act 1999* or *Youth Justice Act 1992*.
The department expects CSPs to be aware of any legislation relevant to the performance of their contractual obligations.

Privacy breaches

Privacy breaches may be accidental or deliberate; they may involve the information of one person or many. For example, an email may be sent to the wrong address or the CSP's computer system could be hacked.

In all cases, it is important that CSPs take immediate containment action and do a risk assessment, so that any potential harm can be prevented or minimised.

The CSP must assess whether to notify affected persons. The department must also be notified as soon as possible. However, the CSP remains responsible for the breach, including taking appropriate remedial action and dealing with any complaints.

The department cannot provide advice and the CSP should consider seeking independent advice about how to respond.

The IP Act does not impose a mandatory obligation to notify the OIC about a privacy breach. However, the OIC strongly encourages organisations to do so. Not only can they provide advice about how to respond to the breach, notification can also assist them respond to any community enquiries about the breach.

The OIC has published guidance about how to respond to breaches.

Complaints

If a person alleges that a bound CSP has breached an IPP or section 33 in relation to their personal information, it is the CSP's responsibility to deal with the complaint.

The OIC has published guidance about how to respond to complaints.

If the complainant is not satisfied with the CSP's response or they do not receive a response within 45 business days, they may

[4] *A 'health agency' is required to comply with the National Privacy Principles (NPPs) set out in schedule 4 of the IP Act. However, the department is not a health agency, and this fact sheet does not discuss the NPPs.*

refer their complaint to the OIC, who will assess whether the matter can be mediated.

The OIC has published guidance about steps the OIC takes when a complaint is referred to it What to expect when OIC receives a privacy complaint - A guide for agencies | Office of the Information Commissioner Queensland

If the complainant is not satisfied with the outcome of that process, they may ask the OIC to refer the matter to the Queensland Civil and Administrative Tribunal (QCAT) for decision. If QCAT finds that the complaint, or a part of it, has been substantiated, it may make a variety of orders, including an order that the CSP pay compensation of an amount up to $100,000 per breach.

Because a privacy breach or complaint may expose the CSP to liability, we recommend that CSPs seek independent legal advice, as appropriate.

The Information Privacy Principles (IPPs)

The IPPs set out how personal information is to be collected, handled, used and disclosed. Refer to the IP Act for the full requirements but below is a summary of the 11 IPPs.

IPP 1 – Collection of personal information must be lawful, fair, and necessary for your organisation's functions.

It is important to analyse what information you require to perform your functions. It does not include information that would be 'nice to know' or might be useful in future.

IPP 2 – Where you ask an individual to provide personal information, you must take all reasonable steps to advise them of the purpose of the collection, any laws which give you authority to collect the information, and to whom you usually disclose or give the information.

Note: An IPP2 notice may be given orally or in writing. If the collection is in writing, a written notice is usually more appropriate.

IPP3 – Personal information you collect must be relevant, up-to-date and complete. The collection must not be an unreasonable intrusion into the personal affairs of the individual.

IPP 4 – You must ensure personal information is protected against loss, unauthorised access or other misuse. The safeguards must be *'adequate to provide the level of protections that can reasonably be expected to be provided'*.

Consider whether your agency has appropriate policies and procedures for–

- *physical security, including secure work areas*
- *management of hard copy files (e.g. secure storage, clean desk policy)*
- *removing work information/devices, from the office and protecting them from loss or theft*
- *conducting interviews in private.*

It is also important to consider whether your organisation has appropriate digital security. This is particularly important if you use cloud-based services.

Tailored guidance is available for small and medium businesses and large organisations on the Australian Cyber Security Centre website Australian Government Information Security Manual (ISM) | Cyber.gov.au

IPP 5 – You must ensure individuals can find out what information you hold about them.

You can do this by publishing a guide about the type of information your organisation collects and how you use or disclose it.

IPP 6 – You must give individuals access to their personal information unless a law allows for refusal.[5]

IPP 7 – An individual has the right to require correction or amendment of their personal information if it is inaccurate, irrelevant, incomplete, out of date or misleading.

IPP 8 – Before using[6] personal information, you must take reasonable steps to ensure it is accurate, complete and up to date.

IPP 9 – You must only use personal information that is directly relevant to the purpose for which it was collected.

IPP10 – You may only use personal information for its original intended purpose, unless one of the listed exceptions applies.

IPP11 – You may only disclose personal information to the person it relates to unless one of the listed exceptions applies.

[5] For example, the IP Act provides that access may be refused to information that is exempt from disclosure or contrary to public interest (Chapter 3 of the IP Act, and the *Right to Information Act 2009*, schedules 1-4.)

[6] Section 23 of the IP Act defines 'use' and 'disclosure' for purposes of IPPs 10 and 11.