Simpson Grierson

Privacy Act – Summary sheet

How does the Privacy Act affect you?

The Privacy Act 2020 controls how agencies collect, use, store, disclose and give access to personal information.

If your organisation faces frequent requests from customers for information it needs a consistent approach in responding to requests for access.

The Information Privacy Principles

The Privacy Act establishes 13 Information Privacy Principles (IPPs) that govern the collection, storage, security, accuracy, retention, use and disclosure of personal information.

The IPPs set out general principles that are subject to a number of exceptions, such as where the information is publically available or specific authorisation is obtained from the individual concerned.

Collection

Principle 1: Information must be collected for a lawful purpose connected with a function or activity of the agency, and be necessary for that purpose (and if such purpose does not require the collection of an individual's identifying information, the agency may not require the individual's identifying information).

Principle 2: Agencies must collect the information directly from the individual concerned. Exceptions include publically available information.

Principle 3: When collecting personal information directly from the individual concerned, agencies need to ensure that the individual is aware of matters such as:

- the **fact** it is being collected;
- the **purpose** of collection;
- intended **recipients;**
- your organisation's **name and contact details;**
- if collection is required/authorised by law, what law and whether supplying that information is **mandatory or voluntary;**
- the **consequences** (if any) for the individual if all or any of the requested information is not provided;
- rights of **access to/correction** of information under the Act.

Principle 4: An agency must not collect information by unlawful, unfair or unreasonably intrusive means (especially where information is collected from children or young persons).

TIP: The purpose for which information is collected is an important concept that runs through the Privacy Act. It is relevant to a number of IPPs. Every time you deal with personal information keep in mind the purpose for which it was collected.

Storage & Security

Principle 5: Personal information must be protected by security safeguards against loss, unauthorised access, use modification or disclosure, or other misuse. The security safeguards must be what is reasonable in the circumstances.

TIP: Develop written employee policies and provide regular privacy training. Don't allow personal information to be taken off-site without appropriate security measures in place. Prohibit discussion of work matters involving personal information with family and friends, or in public.

Access & Correction

Principle 6: Individuals have a right to know if information is held about them and to access that information. Limited reasons to refuse access are set out in sections 49-53 of the Privacy Act, and include where:

- disclosure would pose a serious threat to the life, health, or safety of any individual or to public health or public safety;
- the information is evaluative material, and it would breach confidence to disclose;

- prejudice the maintenance of law or security or defence of New Zealand;
- disclosure would result in disclosure of a trade secret, or unreasonable prejudice to the commercial position of the person who supplied or is the subject of the information;
- the information requested does not exist or cannot be found;
- disclosure would involve an unwarranted disclosure of the affairs of another individual or deceased person;
- the request for disclosure is frivolous or vexatious, or the information requested is trivial.

If an access request is declined, and the matter is referred to the Privacy Commissioner, the Commissioner has the power to direct an agency to provide access to the information.

Principle 7: Individuals have the right to request correction of information about themselves. If you don't agree with the correction requested, you can be asked to have the information flagged with the correction requested but not made.

TIP: Before releasing any personal information check carefully for personal information of other people, or irrelevant but sensitive information. Consider whether any reasons to refuse access apply, and redact parts of documents if necessary.

Accuracy & Retention

Principle 8: Information held must be accurate, up to date, complete, relevant and not misleading.

Principle 9: Information must not be kept for longer than is required for the purposes for which the information may lawfully be used.

Use & Disclosure

Principle 10: Generally personal information should only be used for the purpose for which it was collected (or a directly related purpose).

Principle 11: Generally personal information should not be disclosed unless one of the specified exceptions apply - eg the disclosure is for the purpose for which the information was collected (or a directly related purpose).

Principle 12: Limits disclosure of personal information to a foreign person or entity, to situations where certain safeguards exist (as listed in IPP 12). These include where the information will be protected by comparable safeguards as those under the Act.

TIP: Before disclosing check carefully for personal information of others, or irrelevant but sensitive information. Don't offshore personal information unless you are confident adequate safeguards exist, that are compliant with IPP 12.

Complaints & Offences

If a breach of an IPP results in loss to an individual or has some other adverse effect on the individual, it could be an interference with privacy, and could become the subject of a complaint to the Privacy Commissioner and possibly the Human Rights Review Tribunal. Damages of up to $350,000 can be awarded by the Tribunal. There are a number of offences under the Act that could result in fines of up to $10,000, on conviction. These include obstructing or failing to comply with a requirement of the Privacy Commissioner, impersonating someone in order to access that person's personal information and destroying a document containing personal information knowing it is the subject of a privacy request.

Privacy Officer

Every agency is required to have one or more individuals who are responsible for ensuring the agency's compliance with the Privacy Act, dealing with requests under the Act, and working with the Privacy Commissioner in respect of any investigation under the Act.

Data Breach Notification

If an agency suffers a privacy breach that has, or is likely to, cause serious harm to affected individuals, it is mandatory to report the breach to the Privacy Commissioner, and in some cases, to the affected individuals. Failure to do this could result in a fine of up to $10,000.

TIP: Ensure that you have a policy and appropriate internal systems for mandatory data breach notification.

Contacts

Jania Baigent – Partner
M: 021 550 554
E: jania.baigent@simpsongrierson.com

Karen Ngan – Partner
M: 021 648 977
E: karen.ngan@simpsongrierson.com

Sally McKechnie – Partner
M: 021 180 7236
E: sally.mckechnie@simpsongrierson.com

Carl Blake – Special Counsel
M: 021 477 228
E: carl.blake@simpsongrierson.com