NEXT GENERATION RISK MANAGEMENT

NATIONAL PRIVACY PRINCIPLES COMPLIANCE

SASSI®

Version 1.4, 2017

Document History and Version Control	Date Approved	Approved by	Brief Description
1.0	8 April 2014	Software Development Manager	Creation of original document.
1.1	27 May 2015	Software Development Manager	Minor amendment to add Trade licences and permits in the section NPP1 Collection.
1.2	24 September 2015	Software Development Manager	Change to order of paragraphs.
1.3	21 March 2017	Software Development Manager	Updated links and changes to file format.
1.4	12 September 2017	Software Development Manager	Updated IP Info (Logo and SASSI ®).

Compliance SASSI® System with the National Privacy Principles

See below for a summary of the NPPs according to the Australian Government Australian Information Commissioner's "Guide to Privacy for Small Business" and SASSI Web's compliance comments.

Principle	Description	SASSI® Web Comment
NPP1 Collection	• Only collect personal information that is necessary for your functions or activities. • Use fair and lawful ways to collect personal information. • Collect personal information directly from an individual if it is reasonable and practicable to do so. • At the time you collect personal information or as soon as practicable afterwards, take reasonable steps to make an individual aware of: o why you are collecting information about them; o who else you might give it to; and o other specified matters. • Take reasonable steps to ensure the individual is aware of this information even if you have collected it from someone else.	The only personal information that SASSI collects about an individual is their: • Name • Business email address • Business phone number • Business mobile number • Trade licences • Permits This information is used to contact the person in relation to the business they have with the SASSI® system. As soon as a person's details are collected they are advised by email.
NPP 2 Use and Disclosure	Only use or disclose personal information for the primary purpose of collection unless one of the exceptions in NPP 2.1 applies (for example, for a related secondary purpose within the individual's reasonable expectations, you have consent or there are specified law enforcement or public health and public safety circumstances). Note that: If the information is sensitive the uses or disclosures allowed are more limited. A secondary purpose within reasonable expectations must be directly related to the purpose of collecting the information and the direct marketing provisions of NPP 2.1(c) do not apply.	SASSI® Web complies with this guideline.
NPP 3 Quality	Take reasonable steps to ensure the personal information you collect, use or disclose is accurate, complete and up-to-date. This may require you to correct the information.	SASSI® Provides access to an individual's information so they can ensure it is correct and amend where required.

NPP 4 Security	Take reasonable steps to protect the personal information you hold from misuse and loss and from unauthorised access, modification or disclosure. Take reasonable steps to destroy or permanently de-identify personal information if you no longer need it for any purpose for which you may use or disclose the information.	Personal information of clients' personnel can only be accessed by the individual, an authorised administrator with the client's company or a person from SASSI® who is authorised to add or change individuals' information. Access is controlled by username, password and role.
NPP 5 Openness	Have a short document that sets out clearly expressed policies on the way you manage personal information and make it available to anyone who asks for it. If an individual asks, take reasonable steps to let them know, generally, what sort of personal information you hold, what purposes you hold it for and how you collect, use and disclose that information.	This document will be provided.
NPP 6 Access	If an individual asks, you must give access to the personal information you hold about them unless particular circumstances apply that allow you to limit the extent to which you give access – these include emergency situations, specified business imperatives and law enforcement or other public interests.	All individuals have access to their own information through the SASSI® system.
NPP 7 Identifiers	Only adopt, use or disclose a Commonwealth Government identifier if particular circumstances apply that would allow you to do so.	SASSI® does not use Commonwealth Government identifiers of individuals.
NPP 8 Anonymity	If it is lawful and practicable to do so, give people the option of interacting anonymously with you.	SASSI® does not provide for anonymous interaction.
NPP 9 Transfer overseas	Only transfer personal information overseas if you have checked that you meet the requirements of NPP 9.	SASSI® does not transfer information about individuals overseas.
NPP 10 Sensitive information	Get consent to collect sensitive information unless specified exemptions apply.	SASSI® does not collect sensitive information, according to the NPP's "Meaning of Terms". See below

Meaning of Terms

Access - This involves a small business giving an individual information about themselves held by the small business. Giving access may include allowing an individual to inspect personal information or giving a copy of it to them.

Benefit, Service or Advantage - This includes income, financial concessions, subsidies or some other return to the small business. For example, where a small business sells its customer list to a marketing company or gives its own list in return for another list.
For more information see: https://www.oaic.gov.au

Collection - A small business collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when a small business keeps personal information it has come across by accident or has not asked for.

Commonwealth Contracted Service Provider - This means small businesses that provide services to Commonwealth agencies under contract or subcontract. The *Privacy Act 1988* does not apply to contracts small businesses may have with State or territory governments.

Consent - People must understand what they are agreeing to and agree voluntarily. The consent is not valid or acceptable if there is extreme pressure or coercion, for example, where consent is given under threat.

Consent can be express or implied

> *Express consent:* given explicitly, verbally or in writing.
> *Implied consent*: consent may reasonably be understood in the circumstances from the conduct of the person and the small business.

Contractors - Under the Privacy Act, acts and practices of employees (and those 'in the service of' a small business) in performing their duties of employment are treated as those of the small business (see s 8(1)(a)).

This does not usually apply to contractors performing services for a small business unless there is a particularly close relationship between a small business and a contractor. In that case, the actions of the contractor could be treated as having been done by the small business for the purposes of section 8 of the Privacy Act.

If the small business and the contractor are regarded as separate entities under the Privacy Act, a small business that gives personal information to a contractor is disclosing information and the contractor is collecting the information. This means that for a small business to comply with the NPPs it may need to have clauses in the contract to protect the personal information the small business discloses to the contractor.

Where the contractor is not a 'small business' under the Privacy Act and is not covered by the NPPs it would be advisable for the small business to take steps to protect the personal information it discloses to the contractor.

For more information about how the NPPs apply where a small business contracts out a function or activity to a separate entity see Information Sheet 8-2001 Contractors.
Found at: https://www.oaic.gov.au/privacy-law/privacy-archive/privacy-resources-archive/information-sheet-private-sector-8-2001-contractors

Disclosure - In general terms a small business discloses personal information when it releases it to others outside the small business. It does not include giving individuals information about themselves (this is 'access' see above).

Health Service Provider - Health includes physical, emotional, psychological and mental health. Health service providers: assess, record, maintain or improve a person's health; diagnose or treat a person's illness or disability; or dispense on prescription a drug or medicinal preparation by a pharmacist.

Personal Information - The Privacy Act says personal information means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. This includes information or an opinion forming part of a database. The information may or may not be true (s 6).

Privacy Codes - The NPPs are the default rules which organisations and businesses must comply with. Some organisations and businesses may choose to develop their own Privacy Codes which replace the NPPs. Privacy Codes must meet strict standards in the Privacy Act and be approved by the Privacy Commissioner.

More information can be found at: https://www.oaic.gov.au

Related Body Corporate (*Corporations Act 2001* s 50) - The Privacy Act defines related body corporate by reference to the Corporations Act. Companies might be related where they are a holding company or a subsidiary of another body corporate.

Residential Tenancy Database - The *Privacy (Private Sector) Amendment Regulations 2007* (No.3) states that a residential tenancy database means a database:

that stores personal information in relation to an individual's occupation of residential premises as a tenant; and

that can be accessed by a person other than the operator of the database or a person acting for the operator.

Sensitive Information - Special rules apply to the handling of sensitive information. Sensitive information is a subset of personal information. It is information or opinion about a person and includes:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual preferences or practices;
- criminal record or health information about an individual.
- genetic information that is not health information.

Trading in Personal Information - Trading in personal information happens where businesses collect or disclose an individual's personal information for a "benefit, service or advantage"(see above), for example they buy or sell a list of personal information for income, concessions or some other return. The Act does not prevent trading in personal information but does set principles that need to be followed.

The Privacy Act will not apply where the trading happens with the consent of the individual concerned or is authorised or required by law.

Note: In some circumstances sale of the assets of a business that include personal information will also be trading in personal information.

Use - In general terms, use of personal information refers to the handling of personal information within a small business including 'the inclusion of information in a publication.