galexia

&

Doll Martin Associates

Information and Privacy Commission NSW (IPC)

Privacy Impact Assessment (PIA) for the IPC GIPA Tool

FINAL

(DMA 2016_034)

August 2016

Contact: Doll Martin Associates
Level 18, 323 Castlereagh St, Sydney NSW 2000
Ph: +61 2 9211 6200
Email: manage@dollmartin.com.au

Document Control

Client

This document has been written for the Information and Privacy Commission NSW (the IPC).

Document Purpose

This document is a high level Privacy Impact Assessment for the IPC GIPA Tool. (GIPA is the Government Information (Public Access) Act 2009).

Document Identification

Document title	NSW IPC - Privacy Impact Assessment - GIPA Tool (FINAL - August 2016)
Document filename	DMA_2016_034_NSW_IPC_GIPA_PIA_v9_20160815_FINAL.docx
Document date	15/08/2016 1:51 PM

Client Details

Client Contacts	Roxane Marcelle-Shaw Director, Investigation and Reporting Information and Privacy Commission NSW Level 17, 201 Elizabeth Street, Sydney 2000 Ph: (02) 8071 7020 | mob: 0477 350 273

Consultant Details

Consultant Contact	Peter van Dijk (General Manager) Doll Martin Associates and Galexia Level 18, 323 Castlereagh St, Sydney NSW 2000 Phone: +612 9211 6200 Email: manage@dollmartin.com.au Mobile: +61 419 351 374 (Peter van Dijk)
Document Authors	Doll Martin Associates & Galexia
Reference	DMA 2016_034

Confidentiality

The contents of this document are commercial-in-confidence and based on methods and materials that are proprietary to Galexia. The Client is requested to ensure that it is not given to actual or potential clients or competitors of Doll Martin Associates & Galexia.

Copyright

Contents

1. Executive Summary

Doll Martin Associates (in conjunction with Galexia) is conducting a high level Privacy Impact Assessment (PIA) for the NSW IPC on the IPC GIPA Tool. (GIPA is the Government Information (Public Access) Act 2009).

This review is current as at July 2016.

1.1. Broad Purpose

This Privacy Impact Assessment (PIA) considers the privacy issues raised by the current implementation of the IPC GIPA Tool.

The broad purpose of this privacy review is to:

- Determine whether data collected and stored in the GIPA Tool should be considered personal information;
- Identify any immediate privacy compliance issues;
- Identify any potential future issues; and
- Assist the NSW IPC develop a work plan and priorities for the ongoing governance of privacy issues in the development and implementation of the GIPA Tool.

1.2. Information considered

Information contained in this privacy review is based on:

- Meetings and teleconferences with the NSW IPC;
- Limited engagement with internal stakeholders;
- Review of relevant privacy legislation, notably the NSW Privacy and Personal Information Protection Act 1998 (PPIP Act);
- Consideration of best practice approaches and guidance in other jurisdictions for some key areas where the NSW legislation is silent. This includes Commonwealth guidelines on data breach notification requirements;
- Technical and business documentation related to the GIPA Tool context;
- High level review of information flows;
- Consideration of relevant proposals for future changes to the tool;
- Review of the agreement with Salesforce;
- IPC privacy compliance and governance documentation, including privacy policies and relevant record keeping policies; and
- Relevant guidelines from the NSW Information Commission, NSW IPC and privacy regulators and Government agencies.

1.3. Findings and Recommendations

This Privacy Impact Assessment has identified a number of privacy issues that may require further consideration by the NSW IPC.

Most of the recommendations in the review are suggested enhancements to current policies and procedures, or suggested paths of action related to the implementation of the GIPA Tool.

The key findings and recommendations are set out in the following table, with cross references to each section of the report.

#	Privacy issue	NSW Principle	Finding	Recommendation
R1	**Is the data personal information?** Refer to section 4 at page 11.		The data contained in numerous entry fields in the GIPA Tool should be categorised as personal information for the purpose of compliance with the PPIP Act. A small number of data fields may need to be treated as sensitive information or health information.	No action required.
R2	**Collection** Refer to section 5 at page 13.	IPP1. Lawful	The data collected in a typical GIPA application is being collected for the lawful purpose of processing the application. It is voluntarily submitted by the applicant, and is very low risk data. Some data related to financial hardship is higher risk data, but it is required in order to process a discount for applicants who cannot afford the application fee. Section 42 of the GIPA Act provides a legislative requirement for an application to include, amongst other things, submissions on public interest considerations, request for discount including evidence of hardship, and any other information that the applicant thinks may be necessary. However, some data on country of birth and language spoken falls into the category of sensitive data. This data may be collected by agencies in order to comply with their own legislative requirements for monitoring access and equity issues.	Review the collection of data on country of birth and language, as although it is lawful, it does not appear to be necessary, and it raises additional issues regarding the use of sensitive information. We note that the NSW IPC is already considering removing this data from the GIPA Tool, but it is unclear whether this would include the removal of existing data in the GIPA Tool database.
R3	**Collection** Refer to section 5 at page 13.	IPP2. Direct	Data is generally only collected from the applicant. There are some rare exceptions – for example the Department of Education allows parents to access data related to their children.	No action required.
R4	**Collection** Refer to section 5 at page 13.	IPP3. Open	A typical agency privacy policy does not include any information regarding the specific nature of data collection related to GIPA applications. It does however provide a broad overview, including access and correction rights. GIPA access request application forms usually include a very short privacy notice. The combination of the broad privacy policy and the short privacy notice is sufficient to meet the openness principle, especially when the low risk nature of the data is taken into consideration. However, many agencies do not include any privacy notice on their GIPA application form.	No action required.

#	Privacy issue	NSW Principle	Finding	Recommendation
R5	**Collection** Refer to section 5 at page 13.	IPP4. Relevant	The majority of the data fields are clearly relevant. They are required in order to process the application or to offer a fee discount. However, some data on country of birth and language spoken appears to be less relevant to the overall GIPA objectives. However, this data may be necessary specific agency purposes. The IPC is currently reviewing the GIPA Tool and has recommended removing these categories of data.	Review the collection of data on country of birth and language, as it does not appear to be relevant. We note that the NSW IPC is already considering removing this data from the GIPA Tool, but it is unclear whether this would include the removal of existing data in the GIPA Tool database.
R6	**Storage** Refer to section 6 at page 15.	IPP5. Storage	The application is hosted by Salesforce. Salesforce is 'hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders'. Most data that is likely to identify individuals is encrypted in transit and at rest, although there are some exceptions. Also, the notes fields are not encrypted and may potentially hold personally identifying information. However, encryption is only one layer of security protection, and the overall security standards applied to the data are high. A Cloud Risk Assessment ensuring compliance with DOJ and State Government security practices was conducted. A full audit log of all database access and activity is maintained.	No action required.
R7	**Access and Accuracy** Refer to section 7 at page 16.	IPP6. Transparent	The GIPA Tool is not a consumer facing application. The only users are agency staff. Some general information, including a user manual, is available on the NSW IPC website. Applicants are likely to have no direct contact with the GIPA Tool – their interactions are with individual agencies. Each agency has a broad privacy policy and usually adds a very short privacy notice to their GIPA Application form. The combination of these three items, is sufficient to ensure compliance with the transparency principle. It would be overkill to develop a specific privacy policy just for the GIPA Tool. A minor compliance issue is that the NSW IPC Privacy Management Plan (June 2014) states that the GIPA Tool is hosted by RMS. This information needs to be updated.	No significant action is required. A minor compliance issue is that the NSW IPC Privacy Management Plan (June 2014) needs to be updated to reflect the current hosting arrangement. This requirement has been acknowledged by the NSW IPC.
R8	**Access and Accuracy** Refer to section 7 at page 16.	IPP7. Accessible	There are two ways that applicants can access their data. First, they can contact the relevant agency and ask for access. Most agencies provide both informal and formal mechanisms for processing such requests. Secondly, consumers can contact the IPC for assistance. This would normally only happen if they were unsatisfied with the agency response. These two processes for access are clearly disclosed in agency privacy policies and in information for consumers on the IPC website.	No action required.

#	Privacy issue	NSW Principle	Finding	Recommendation
R9	**Access and Accuracy** Refer to section 7 at page 16.	IPP8. Correct	There are two ways that applicants can correct their data. First, they can contact the relevant agency and ask for a correction. Most agencies provide both informal and formal mechanisms for processing such requests. Each agency can correct data for applicants, by directly accessing the GIPA Tool database. Secondly, consumers can contact the IPC for assistance. This would normally only happen if they were unsatisfied with the agency response. These two processes for correction are clearly disclosed in agency privacy policies and in information for consumers on the IPC website.	No action required.
R10	**Use** Refer to section 8 at page 18.	IPP9. Accurate	This is a high level privacy review – there has not been an opportunity to examine any specific data quality issues or data quality control measures. Sections 41, 51 and 52 of the GIPA Act provide legislative requirements for validity. This means the data is assessed and quality assured as part of the application process. Applicant data is only used in the GIPA Tool for processing the application and contacting the applicant with the results, so there are numerous opportunities for the applicant to correct any information. Data is not generally used or disclosed for any other purposes.	Not assessed in detail in this review.
R11	**Use** Refer to section 8 at page 18.	IPP10. Limited	Applicant data is only used in the GIPA Tool for processing the application and contacting the applicant with the results. Some data is used for processing fee discounts. Personal information is not used for other purposes. For example, there are no secondary uses of the data that require the inclusion of personal information – the annual reporting requirements can be met by using anonymous, aggregated data.	No action required.
R12	**Disclosure** Refer to section 9 at page 19.	IPP11. Restricted	Personal information held in the GIPA Tool is not generally released. If a request was received for the release of personal information the request would be processed by the relevant agency or the NSW IPC in accordance with the GIPA Act, the agency privacy policy, the agency privacy management plan, and the PPIP Act (subject to the requirement of the GIPA Act which may exclude information in certain circumstances). The other relevant aspect of Principle 11 is that the data has been 'released' to Salesforce for their role in hosting the GIPA Tool. It is clear that this release is a related purpose and the applicant is unlikely to object. The GIPA Tool is a 'background process' that is well within consumer expectations of administrative processing functions for data of this type.	No action required.

#	Privacy issue	NSW Principle	Finding	Recommendation
R13	**Disclosure** Refer to section 9 at page 19.	IPP12. Safeguarded	The current GIPA Tool does include the collection of data on country of birth, and language spoken. These fields are not mandatory, but we assume that some of this data has been entered. The information has never been released beyond the GIPA Tool, but the information is now located on the Salesforce platform. The relevant individuals have not provided explicit consent to the release of this sensitive information – the typical GIPA application form only includes a very short privacy notice. The IPC is currently reviewing the GIPA Tool and has recommended removing these two categories of data. If this recommendation is implemented, it may need to be extended to the removal of existing data in these two categories. In addition, prior versions of the GIPA Tool may have collected specific data on Aboriginal and Torres Strait islander applicants. This field was removed in June 2016, but it is unclear whether any existing data has been retained. This issue should be explored further, with a view to removing any data on Aboriginality that is stored in the GIPA Tool database.	Consider the removal of sensitive data fields from the GIPA Tool, including the removal of existing data from the GIPA Tool database.
R14	**Cross border transfer** Refer to section 10 at page 20.		Data can be transferred outside NSW (e.g. to the Salesforce cloud platform) relying on the contract where Salesforce have agreed to be bound by the NSW Information Protection Principle. This contract provides an effective method of upholding compliance with the Principles.	No action required.
R15	**Data breach notification** Refer to section 11 at page 21.		At this stage there is no data breach response plan in place for the GIPA Tool, although Salesforce has a generic data breach response plan in place for their overall service. The NSW IPC could consider taking responsibility for the development of a specific GIPA Tool data breach response plan. This is not an urgent requirement, but it does reflect emerging best practice.	No immediate action required. In the medium term, the NSW IPC could consider taking responsibility for the development of a specific GIPA Tool data breach response plan.

2. Scope and Methodology

Doll Martin Associates (in conjunction with Galexia) has prepared this high-level Privacy Impact Assessment (PIA) utilising the structure of the short form PIA Template published by the Commissioner for Privacy and Data Protection Victoria in 2015. However, the content has been customised for compliance with relevant NSW legal provisions.

As this is a high level PIA, the assessment is based on compliance with the 12 broad Principles in the NSW legislation, rather than the detailed legislative requirements. The PIA also includes some advice on best practice in areas where the NSW legislation is silent.

The scope of this privacy review is limited to the following items:

In Scope	Out of Scope
• High level identification of potential compliance issues in the context of the NSW privacy legal framework,	• Compliance with specific sectoral legislation
• Brief review of *key* documents related to the IPC GIPA tool	• Review of the entire suite of NSW IPC documentation
• Very limited stakeholder consultation (internal staff members by email and phone)	• Extensive stakeholder consultation, or assessment of public attitudes etc.
• Brief review of existing security assessment	• Full security audit
• High level identification and review of legal documentation	• Detailed legal advice

3. Description of the GIPA Tool

The Government Information Privacy Act 2009 (GIPA) requires the Information and Privacy Commission (IPC) to provide a resource to assist agencies in processing GIPA applications and to report annually on the operation of GIPA.

In order to facilitate these requirements the IPC has developed and implemented a case management and reporting system called the 'GIPA Tool'. The GIPA tool was originally developed and hosted by the RMS in conjunction with an outsourced contractor (Fujitsu), but has recently moved to a cloud services platform, provided by Salesforce.

The key features of the current implementation of the GIPA Tool are:

- Use is not mandatory, but there are numerous registered users (200-300 agencies in 2016);
- Many agencies are using it for their annual reporting requirements; and
- Use is particularly popular amongst local councils.

The key functionality of the GIPA Tool includes the following:

- Facility for agencies to case manage GIPA applications in compliance with legislative obligations;
- Facilitate reporting for individual agencies;
- Facility for agencies to add GIPA applications;
- Facility for agencies to edit GIPA applications;
- Facility for agencies to search GIPA applications;
- Pre-configured tables as specified in Schedule 2 of Government Information (Public Access) Regulations 2009 (GIPA Regulations); and
- Reporting and charting tool functionality.

The GIPA Tool is the subject of regular reviews and improvements – it is a very dynamic application. More information on the GIPA Tool, including user guides, is available at: <http://www.ipc.nsw.gov.au/ipc-gipa-tool>.

4. Is the data 'personal information'?

4.1. The Law

In NSW Privacy and Personal Information Protection Act 1998 (PPIP Act) personal information means 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'. (Section 4 (1))

Personal information is deemed to be 'held' by a public sector agency if:

> (a) the agency is in possession or control of the information, or
>
> (b) the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or
>
> (c) the information is contained in a State record in respect of which the agency is responsible under the State Records Act 1998. (Section 4 (4))

The PPIP Act includes some additional provisions and exceptions, but these are not relevant to the type of information collected in the GIPA Tool.

The Act also contains some special rules for 'sensitive' personal information:

> 19. Special restrictions on disclosure of personal information
>
> (1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

4.2. GIPA – Overview

GIPA applications are made by a range of individuals, including members of the public, journalists, Members of Parliament and researchers. The requests are made to individual agencies, typically on an official application form.

The GIPA Tool is used by agencies to manage the high level data collection and annual reporting requirements related to these applications. The GIPA Tool only includes information that describes the application – it does not include data that is the *subject* of the application. As a result, the GIPA Tool database only includes personal data associated with the applicant. This data is entered into the GIPA Tool by each agency.

Information on GIPA applicants is not seen by the IPC unless the application relates to the IPC itself (this is rare, and is outside the scope of this PIA).

The GIPA Tool includes the following fields that may include personal information related to the applicant:

Field Name	Encrypted	Mandatory
First Name	Yes	Yes
Surname	Yes	Yes
Type of applicant	No	Yes
Address line 1	Yes	Yes
Address line 2	Yes	No

Field Name	Encrypted	Mandatory
Suburb	Yes	Yes
State	Yes	Yes
Postcode	Yes	Yes
Home phone	Yes	No
Work phone	Yes	No
Mobile	Yes	No
Fax	Yes	No
Email address	Yes	No
Country of birth [subject to current review]	Yes	No
Main language spoken [subject to current review]	No	No
Aboriginal or Torres Strait Islander [removed in June 2016]	Yes	No
Does the applicant have any special needs?	No	No

There is also a general ‘notes’ field that may contain personal information.

As can be seen in the table, many of the data fields contain personal information. The cumulative effect of this data means that the individual can be easily identified.

Some of the data fields may contain sensitive personal information, such as information related to language and country of birth. Not all of the fields are mandatory, but for the purposes of this PIA we assume that some sensitive personal information is likely to be collected in these fields.

One field may also contain minor examples of personal ‘health information’, as there is a question related to the special needs of the applicant. This field is not mandatory, but id helpful for managing client needs (e.g. providing documents in a format that is accessible).

4.3. ‘Personal information’ finding

The data contained in numerous entry fields in the GIPA Tool should be categorised as personal information for the purpose of compliance with the PPIP Act. A small number of data fields may need to be treated as sensitive information.

5. Collection of personal information (IPP1-4)

5.1. The Law

The PPIP Act contains four principles on the collection of personal information. They are summarised in the following section.

5.2. GIPA – Overview

Principle	Collection	Notes	Y	N
IPP1	**Lawful** Does the program only collect personal information for a lawful purpose. It must be needed for the agency's activities?	The data collected in a typical GIPA application is being collected for the lawful purpose of processing the application. It is voluntarily submitted by the applicant, and is very low risk data Some data related to financial hardship is higher risk data, but it is required in order to process a discount for applicants who cannot afford the application fee. Section 42 of the GIPA Act provides a legislative requirement for an application to include, amongst other things, submissions on public interest considerations, request for discount including evidence of hardship, and any other information that the applicant thinks may be necessary. However, some data on country of birth and language spoken falls into the category of sensitive data. This data may be collected by agencies in order to comply with their own legislative requirements for monitoring access and equity issues. The IPC is currently reviewing the GIPA Tool and has recommended removing these two categories of data.	**PARTIAL**	
IPP2	**Direct** Does the program only collect information from the individual, unless exemptions apply?	Data is generally only collected from the applicant. There are some rare exceptions – for example the Department of Education allows parents to access data related to their children.	**YES**	
IPP3	**Open** Does the program inform individuals that the information is being collected, why and who will be using it and storing it. Individuals must be told how to access it and make sure it's correct?	A typical agency privacy policy does not include any information regarding the specific nature of data collection related to GIPA applications. It does however provide a broad overview, including access and correction rights. GIPA access request application forms usually include a very short privacy notice, for example: **Privacy notice:** The information provided on this application form is being obtained for the purpose of processing your GIPA application. Providing this information is required by law. It will be stored securely. If you do not provide all or any of this information it could prevent or delay the processing of your application. [from EPA at: http://www.environment.nsw.gov.au/resources/whoweare/130802epagipaapp.pdf] The combination of the broad privacy policy and the short privacy notice is sufficient to meet the openness principle, especially when the low risk nature of the data is taken into consideration. However, many agencies do not include any privacy notice on their GIPA application form.	**YES**	

Principle	Collection	Notes	Y	N
IPP4	**Relevant** Is the personal information is relevant, accurate, current and non-excessive?	The majority of the data fields are clearly relevant. They are required in order to process the application or to offer a fee discount. However, some data on country of birth and language spoken appears to be less relevant to the overall GIPA objectives. However, this data may be necessary specific agency purposes. The IPC is currently reviewing the GIPA Tool and has recommended removing these two categories of data.	PARTIAL	

5.3. Collection Finding

Overall, this privacy review has not identified any major issues in relation to the collection of personal information. The following minor actions have been recommended:

- The NSW IPC should review the collection of data on country of birth and language, as although it is lawful, it does not appear to be necessary, and it raises additional issues regarding the use of sensitive information. We note that the NSW IPC is already considering removing this data from the GIPA Tool, but it is unclear whether this would include the removal of existing data in the GIPA Tool database; and
- The NSW IPC should review the collection of data on country of birth and language, as it does not appear to be relevant. We note that the NSW IPC is already considering removing this data from the GIPA Tool, but it is unclear whether this would include the removal of existing data in the GIPA Tool database.

6. Storage (IPP5)

6.1. The Law

The PPIP Act contains one principle on the storage of personal information. The principle is summarised in the following section.

6.2. GIPA – Overview

Principle	Storage	Notes	Y	N
IPP5	Does the program store personal information securely? It should not kept longer than needed, and disposed of properly	The application is hosted by Salesforce. Salesforce is 'hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders'. Most data that is likely to identify individuals is encrypted in transit and at rest, although there are some exceptions to this (see the section above on the definition of personal Information). Also, the notes fields are not encrypted and may potentially hold personally identifying information. However, encryption is only one layer of security protection, and the overall security standards applied to the data are high. A Cloud Risk Assessment ensuring compliance with State Government security practices was conducted. Ongoing security governance includes the maintenance of a full audit log of all database access and activity and regular security audits.	**YES**	

6.3. Storage Finding

Overall, this privacy review has not identified any major issues in relation to the storage of personal information. No specific actions have been recommended.

7. Access and Accuracy (IPP6-8)

7.1. The Law

The PPIP Act contains three principles on access and accuracy. They are summarised in the following section.

7.2. GIPA – Overview

Principle	Access and Accuracy	Notes	Y	N
IPP6	**Transparent** Does the program provide individuals with details about the personal information they are storing, reasons why they are storing it and how individuals can access it if they wish to make sure it's correct?	The GIPA Tool is not a consumer facing application. The only users are IPC and government agency staff, Some general information, including a user manual, is available on the NSW IPC website: http://www.ipc.nsw.gov.au/ipc-gipa-tool Applicants have no direct contact with the GIPA Tool – their interactions are with individual agencies. Each agency has a broad privacy policy and usually adds a very short privacy notice to their GIPA Application form. The combination of these three items (the general information about the GIPA Tool, the broad agency privacy policy, and the short privacy notice on application forms), is sufficient to ensure compliance with the transparency principle. Consumers with additional queries can contact the NSW IPC or the relevant agency for further information. It would be overkill to develop a specific privacy policy just for the GIPA Tool. A minor compliance issue is that the NSW IPC Privacy Management Plan (June 2014) available to the public states that the GIPA Tool is hosted by RMS. This information needs to be updated.	**YES**	
IPP7	**Accessible** Does the program allow individuals to access your personal information in a reasonable time frame and without being costly?	There are two ways that applicants can access their data. First, they can contact the relevant agency and ask for access. Most agencies provide both informal and formal mechanisms for processing such requests. Secondly, consumers can contact the IPC for assistance. This would normally only happen if they were unsatisfied with the agency response. These two processes for access are clearly disclosed in agency privacy policies and in information for consumers on the IPC website.	**YES**	

Principle	Access and Accuracy	Notes	Y	N
IPP8	**Correct** Does the program allow individuals to update, correct or amend your personal information when needed?	There are two ways that applicants can correct their data. First, they can contact the relevant agency and ask for a correction. Most agencies provide both informal and formal mechanisms for processing such requests. Each agency can correct data for applicants, by directly accessing the GIPA Tool database. Secondly, consumers can contact the IPC for assistance. This would normally only happen if they were unsatisfied with the agency response. These two processes for correction are clearly disclosed in agency privacy policies and in information for consumers on the IPC website.	YES	

7.3. Access and Accuracy Finding

Overall, this privacy review has not identified any major issues in relation to access and accuracy. No specific actions have been recommended.

A minor compliance issue is that the NSW IPC Privacy Management Plan (June 2014) needs to be updated to reflect the current hosting arrangement.

8. Use (IPP9-10)

8.1. The Law

The PPIP Act contains two principles on the use of personal information. They are summarised in the following section.

8.2. GIPA – Overview

Principle	Use	Notes	Y	N
IPP9	**Accurate** Does the program ensure sure that personal information is correct and relevant before using it?	This is a high level privacy review – there has not been an opportunity to examine any specific data quality issues or data quality control measures. Sections 41, 51 and 52 of the GIPA Act provide legislative requirements for validity. This means the data is assessed and quality assured as part of the application process. Applicant data is only used in the GIPA Tool for processing the application and contacting the applicant with the results, so there are numerous opportunities for the applicant to correct any information. Data is not generally used or disclosed for any other purposes.	**n/a**	
IPP10	**Limited** Does the program only use personal information for the reason they collected it?	Applicant data is only used in the GIPA Tool for processing the application and contacting the applicant with the results, Some data is used for processing fee discounts. Personal information is not used for other purposes. For example, there are no secondary uses of the data that require the inclusion of personal information – the annual reporting requirements can be met by using anonymous, aggregated data.	**YES**	

8.3. Use Finding

Overall, this privacy review has not identified any major issues in relation to the use of personal information. No specific actions have been recommended.

9. Disclosure

9.1. The Law

The PPIP Act contains two principles on the disclosure of personal information. They are summarised in the following section.

9.2. GIPA – Overview

Principle	Disclosure	Notes	Y	N
IPP11	**Restricted** Does the program only release personal information if the individual has consented? An agency, however, may also release information if it's for a related reason and can be reasonably assumed that the individual would not object, or the information is needed to deal with a serious and impending threat to someone's health and safety.	Personal information held in the GIPA Tool is not generally released. If a request was received for the release of personal information the request would be processed by the relevant agency or the NSW IPC in accordance with the GIPA Act, the agency privacy policy, the agency privacy management plan, and the PPIP Act (subject to the requirement of the GIPA Act which may exclude information in certain circumstances). The other relevant aspect of Principle 11 is that the data has been 'released' to Salesforce for their role in hosting the GIPA Tool. It is clear that this release is a related purpose and the applicant is unlikely to object. The GIPA Tool is a 'background process' that is well within consumer expectations of administrative processing functions for data of this type.	**YES**	
IPP12	**Safeguarded** Does the program not disclose sensitive information without the individual's consent? Such information includes: racial, ethnic information, political, religious and philosophical beliefs, sexual activity and trade union membership. The information may only be released without consent to deal with a serious and impending threat to someone's health and safety.	The current GIPA Tool does include the collection of data on country of birth, and language spoken. These fields are not mandatory, but we assume that some of this data has been entered. The information has never been released beyond the GIPA Tool, but the information is now located on the Salesforce platform. The relevant individuals have not provided explicit consent to the release of this sensitive information – the typical GIPA application form only includes a very short privacy notice. The IPC is currently reviewing the GIPA Tool and has recommended removing these two categories of data. If this recommendation is implemented, it may need to be extended to the removal of *existing* data in these two categories. In addition, prior versions of the GIPA Tool may have collected specific data on Aboriginal and Torres Strait Islander applicants. This field was removed in June 2016, but it is unclear whether any existing data has been retained. This issue should be explored further, with a view to removing any data on Aboriginality that is stored in the GIPA Tool database.	**PARTIAL** Refer to R13 in *Section 1.3.* Findings and Recommendations at page 5.	

9.3. Disclosure Finding

Overall, this privacy review has not identified any major issues in relation to the disclosure of personal information. The following minor action has been recommended:

— The NSW IPC should consider the removal of sensitive data fields from the GIPA Tool, including the removal of existing data from the GIPA Tool database.

10. Cross-border transfer of personal information

10.1. The Law

Section 19.2 of the PPIP Act states that a public sector agency that holds personal information about an individual must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless one of a number of exceptions applies.

The exceptions are set out in the compliance table below.

10.2. GIPA – Overview

Principle	Cross border data transfers	Notes	Y	N
NSW PPIP Act 19.2 (a)	The agency reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles	This is the exception that is most relevant to the Salesforce hosting of the GIPA Tool. Salesforce has signed a contract agreeing to be bound by the NSW Information Protection Principles, and this contract provides an effective method of upholding compliance with the Principles.	**YES**	
NSW PPIP Act 19.2 (b)	The individual expressly consents to the disclosure	Express consent is not required.	**n/a**	
NSW PPIP Act 19.2 (c)	The transfer is necessary for the performance of a contract between the individual and the organisation	Not relevant.	**n/a**	
NSW PPIP Act 19.2 (d)	The transfer is necessary as part of a contract in the interest of the individual between the organisation and a third party	Not relevant.	**n/a**	
NSW PPIP Act 19.2 (e)	All of the following apply: The transfer is for the benefit of the individual; AND It is impractical to obtain consent; AND If it were practicable the individual would likely consent	Not relevant.	**n/a**	
NSW PPIP Act 19.2 (f)	The disclosure is reasonably believed by the public sector agency to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person	Not relevant.	**n/a**	
NSW PPIP Act 19.2 (g)	The organisation has taken reasonable steps so that the information transferred will be held, used and disclosed consistently with the IPPs	This exception also applies to the Salesforce hosting of the GIPA Tool, as the organisation has taken steps [redacted] to ensure compliance.	**YES**	
NSW PPIP Act 19.2 (h)	The disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law.	Not relevant.	**n/a**	

10.3. Cross Border Transfer Finding

Overall, this privacy review has not identified any major issues in relation to the cross border transfer of data. No specific actions have been recommended.

11. Data Breach Notification Requirements

11.1. The Law

NSW does not impose mandatory data breach notification requirements on organisations. However, *voluntary* guidelines are in place at the Commonwealth level:

> OAIC, *Data breach notification — A guide to handling personal information security breaches*, 2014, <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>

There is no current data on the number of organisations who have adopted the voluntary guidelines, but the expectation is that larger organisations with high risk data sets should at least consider adopting the guidelines.

The OAIC guidelines are quite complex, but the best practice requirements are summarised as follows:

— Is there a data breach response plan and does it flow logically from any broader information security plan?

— Is the plan regularly tested?

— Does the plan include a strategy to assess and contain breaches?

— Does the plan clearly identify those actions that are legislative or contractual requirements?

— Are your staff educated about the plan and how to identify and respond to data breaches?

— Does the plan enable staff to identify data breaches and require that breaches be reported?

— Does the plan establish clear lines of command and indicate responsible officers?

— Does the plan outline clearly when affected individuals should be notified of breaches?

— Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?

It is possible that the Australian Government may pass mandatory data breach notification rules at some point in the near future. The issue is the source of ongoing debate in Canberra.

11.2. GIPA Overview

Principle	Data breach notification	Notes	Y	N
Cth	Is there a data breach response plan and does it flow logically from any broader information security plan?	At this stage there is no data breach response plan in place for the GIPA Tool, although Salesforce has a generic data breach response plan in place for their overall service. The NSW IPC could consider taking responsibility for the development of a specific GIPA Tool data breach response plan. This is not an urgent requirement, but it does reflect emerging best practice.		**NO** Refer to R15 in *Section 1.3.* Findings and Recommendations at page 5.
Cth	Is the plan regularly tested?	n/a	**n/a**	

Principle	Data breach notification	Notes	Y	N
Cth	Does the plan include a strategy to assess and contain breaches?	n/a	**n/a**	
Cth	Does the plan clearly identify those actions that are legislative or contractual requirements?	n/a	**n/a**	
Cth	Are your staff educated about the plan and how to identify and respond to data breaches?	n/a	**n/a**	
Cth	Does the plan enable staff to identify data breaches and require that breaches be reported?	n/a	**n/a**	
Cth	Does the plan establish clear lines of command and indicate responsible officers?	n/a	**n/a**	
Cth	Does the plan outline clearly when affected individuals should be notified of breaches?	n/a	**n/a**	
Cth	Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?	n/a	**n/a**	

11.3. Data Breach Notification Requirements Finding

Overall, this privacy review has not identified any major issues in relation to the data breach notification requirements. The following minor action has been recommended:

— In the medium term, the NSW IPC could consider taking responsibility for the development of a specific GIPA Tool data breach response plan.

12. Future Programs and Governance

An ‘End-to-End Review’ of the IPC GIPA Tool is being undertaken to enable the documentation and delivery of a road map for the further development of the IPC GIPA Tool and its functionality.

A discussion paper was released in June 2016, and agencies have been invited to make comments and suggestions. Some of the proposed revisions will have a direct impact on privacy. The following table summarises the most relevant proposals:

Proposed revision	Impact	Notes	Recommendation
A. The Country of Birth field is not required and can be removed	**Positive**	The removal of country of birth reduces the amount of potential sensitive information (racial background) collected in the GIPA Tool.	This proposed revision should be accepted
B. Language spoken field is not required and can be removed.	**Positive**	The removal of language spoken reduces the amount of potential sensitive information (racial background) collected in the GIPA Tool.	This proposed revision should be accepted
C. Aboriginal or Torres Strait Islander check box is not required and can be removed	**Positive**	The removal of the Aboriginality section reduces the amount of potential sensitive information (racial background) collected in the GIPA Tool.	This item was removed in June 2016. However, it is not clear whether existing information captured in this category has been retained.
D. New non mandatory field ‘Proof of Identity’ required. (With selection list e.g. Current Passport, Drivers Licence, Other Proof of Signature and Address details)	**Caution advised**	The addition of any proof of identity information may raise additional privacy risks, especially if the field is ‘open text’. Users may inadvertently add detailed proof of information data to the system (e.g. Passport numbers). It is not clear whether there is any specific requirement beyond noting that identity has been verified.	Careful consideration should be given to this potential revision. If a section on proof of identity is added, additional limits and guidance should be incorporated to prevent the recording of identifiers in the database.
E. Add tick boxes to indicate why a discount was applied. (Options to be: Financial hardship and Special public benefit)	**Caution advised**	Adding information on financial hardship to the database raises a privacy risk that should be assessed against the potential benefits of including this information. Although financial hardship is not a specific category of sensitive data in NSW privacy legislation, it is generally considered to be high risk information (e.g. if the data was disclosed, the consequences for the individual could be serious).	Careful consideration should be given to this potential revision. The consequences of disclosure of this information are significant.