PRIVACY & THE VICTORIAN HOUSING REGISTER

Introduction

Following recent changes to the *Housing Act 1983* (Vic) (**Housing Act**), the Victorian Housing Register (**VHR**) is now available to registered housing agencies in Victoria to access and utilise as a single entry point for all public and community housing vacancies across the state. There are a range of privacy obligations your organisation will need to consider in order to consolidate with the VHR and participate in its ongoing operation. This fact sheet is designed to assist registered agencies get involved in the VHR in accordance with relevant privacy laws.

What does privacy mean?

The *Privacy Act 1988* (Cth) (**Privacy Act**) regulates how personal information is handled. The Privacy Act defines personal information as:

…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

The Australian Privacy Principles (**APPs**) which are contained in the Privacy Act, outline how most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (**APP entities**) must handle, use and manage personal information. Generally speaking, most small businesses with an annual turnover of less than $3 million will not have to comply with the Privacy Act.

Public sector agencies, including contracted service providers, must comply with the *Privacy and Data Protection Act 2014* (Vic) which contains the Information Privacy Principles (**IPPs**) instead of the Privacy Act. The APPs closely align with the requirements under the IPPs however there are some differences so it is important to find out which legislation applies to your organisation.

The APPs place more stringent obligations on APP entities when they handle 'sensitive information'.

Sensitive information is a type of personal information and includes information about an individual's:

- health
- racial or ethnic origin
- political opinions
- membership of a political association, professional or trade association or trade union
- religious beliefs or affiliations
- philosophical beliefs
- sexual orientation or practices
- criminal record.

Under the APPs, entities must put in place reasonable security safeguards and take reasonable steps to protect the personal information that they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.

There are also requirements under APPs in relation to the collection, use, and disclosure of personal information.

Whilst consolidating your organisation's database with the VHR will provide many benefits, your organisation must take into consideration your organisation's obligations under the APPs (and any other relevant privacy legislation) to mitigate the risk of a data breach.

For further information in relation to your organisation's privacy obligations refer to the Office of Australian Information Commissioner website or please contact Cecelia Irvine-So, Principal, of Moores.

How to consolidate your organisation's database with the VHR without breaching privacy?

To consolidate your organisation's database with the VHR, and participate in the VHR, your organisation will need to firstly become a "participating registered agency" by submitting an application in writing to DHHS and the application being approved by DHHS.

Secondly, an "authorised person" within your organisation will need to make your organisation's database available to DHHS. To become an authorised person, a person employed or engaged by a participating registered agency may apply in writing to DHHS for authorisation.

An authorised person can disclose the personal information of applicants to DHHS as part of the consolidation process. The consent of the applicant is not required due to the Housing Act.

A participating registered agency might express a preference to obtain consent from the applicants (or provide them with advance notice) as a courtesy to minimise the risk of applicants being disgruntled about the disclosure of their personal information. You may wish to use words to the effect of:

"[Name of organisation] will soon be consolidating its [waiting list/ register of interest] with the new Victorian Housing Register - the single register for all Victorians seeking public housing and community housing. Accordingly, your personal details which are currently stored on our [waiting list/ register of interest] will be made available to the Department of Health and Human Services so that your application can be added to the Victorian Housing Register. We will be doing this under changes to the Housing Act 1983 (Vic) which facilitate this process. Your application will still be considered for future vacancies with us once this process is complete."

However a participating registered agency is not legally required to obtain consent from the applicants or provide advanced notice.

Are staff members allowed to collect, use and disclose an applicant's personal details once the VHR is operational in your organisation?

Once your organisation becomes a participating registered agency, any person employed by your organisation (known as a "relevant person") may collect or use an applicant's personal details, or disclose an applicant's personal details to another person employed by your organisation, for the following purposes:

- to determine whether an applicant meets the eligibility criteria for social housing;
- to determine which priority category applies to an eligible applicant;
- to determine whether to allocate a tenancy in social housing to an eligible applicant;
- to determine the health, safety and support needs and housing requirements of individuals who are seeking housing assistance;
- to facilitate the management and granting of tenancies in social housing and in other housing to support individuals to access housing that is appropriate to their needs;
- to prepare reports and compile statistics in relation to the use of the VHR;
- to perform any other functions or exercise any power under the Housing Act; and
- to give information that the staff member is otherwise expressly authorised, permitted or required to give under the Housing Act.

Your organisation must also comply with the privacy legislation in relation to the collection, use and disclosure of personal information.

DHHS will be monitoring the use of the VHR database by participating registered agencies and their staff.

Can all staff members in your organisation access the VHR?

Only authorised persons can access the VHR. An authorised person can access the VHR for the following purposes:

(a) to verify the status of an applicant's application for a tenancy in social housing; to maintain the accuracy of the information in the VHR;

(b) to determine whether an applicant meets the eligibility criteria for a tenancy in social housing;

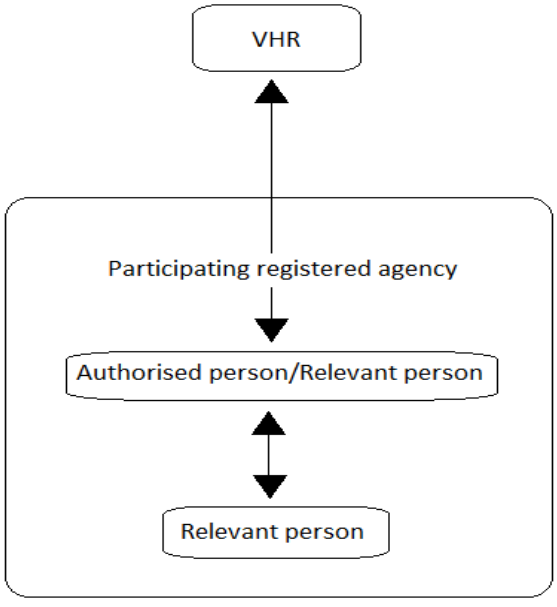
(c) to determine which priority category applies to an eligible applicant;

(d) to determine whether to allocate a tenancy in social housing to an eligible applicant;

(e) to verify the personal details of an applicant or of a household member of an applicant;

(f) to prepare reports and compile statistics in relation to the use of the VHR;

to perform any other function or exercise any power conferred on DHHS or the authorised person, as the case may be.



What happens if an applicant says that they do not want their personal information being stored in the VHR?

Under the APPs, an individual is entitled to access their personal information and request amendments be made. Your organisation must update an individual's personal details if they are inaccurate, incomplete or not up to date. Accordingly, if an applicant decides that they no longer want their personal information to be stored in the VHR this request must be responded to accordingly.

We recommend your organisation include in your privacy policy the extent to which the organisation can service the needs of a person (if at all) in circumstances where they do not want their information stored in the VHR or they want to remain anonymous.

Once the VHR is operational in your organisation, what can your organisation do to ensure that it is complying with the Housing Act as well as relevant privacy obligations?

Your organisation must have in place data security mechanisms to minimise the risk of a data breach occurring.

A data breach occurs when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference. For instance, a data breach may occur when a device containing an applicant's personal information is lost or stolen or an entire database containing personal information is hacked. Even if your company is the hacking "victim", your company will be the party held responsible under privacy law.

In the context of the VHR, there is a risk that a data breach may arise if a person employed by your organisation who is not an authorised person accesses the VHR, or a staff member collects a person's personal details for a purpose not authorised under the Housing Act, or a staff member discloses an applicant's personal details to a person outside the organisation in breach of the Housing Act.

To minimise the risk of a data breach occurring, it is important to do the following:

- Audit your policy and compliance and assess whether there are any security risks associated with the way in which your organisation handles personal information (including health information).
- Formulate a strategy to minimise risk and protect the security of personal information (e.g. include data security as an agenda item in board meetings).
- Review your privacy policy and make any necessary amendments.
- Provide training to your employees (including the response team) about their responsibilities and how to manage personal information.
- Review your data breach response plan and make any necessary amendments or recommendations.

What happens if there is a data breach?

If a staff member of a registered agency breaches the privacy legislation, the staff member must comply with the registered agency's data breach response plan which should include:

- a clear explanation of what comprises a data breach, to enable your employees to readily identify a potential or actual breach;
- a strategy for assessing, managing and containing suspected or confirmed data breaches;
- a clear and immediate communications strategy to allow for prompt notification of affected individuals and other relevant entities (including the OAIC or government funding organisations, if required);
- clear reporting lines and processes for escalation to your organisation's response team;
- how to record data breaches; and
- a system for a post-breach review and assessment of response to prevent future breaches.

A data breach can be extremely costly to your organisation so it is critical to invest in developing a framework in your organisation to ensure that you securely manage personal information and effectively respond to data breaches. The OAIC has the power to issue enforceable undertakings and fines of up to 1.7 million dollars for serious or repeated breaches of privacy. A data breach may also result in reputational damage, put your organisation at risk of losing government funding, and cause stakeholders to lose trust and confidence in your organisation.