PRIVACY DURING RECRUITMENT

The *Privacy and Data Protection Act 2014* (**PDP Act**), contains information privacy protections for personal information that operate during recruitment. The privacy protections in the PDP Act are enshrined in 10 Information Privacy Principles (**IPPs**) that govern how VPS employers must handle any personal information they hold, including that of their employees.

This resource provides general guidance to Victorian public sector (**VPS**) employers on their privacy obligations when undertaking a recruitment process.

COLLECTING PERSONAL INFORMATION FROM APPLICANTS

As part of the application process, employers will generally require applicants to provide a range of information, including personal information such as the applicant’s name, contact details, and employment history.

Under IPP 1.1, VPS employers may only collect personal information if it is necessary for one or more of their functions or activities. As such, employers should initially request no more personal information from applicants than is necessary to assess their suitability for a position or progression to the next stage of the application process.

IPP 1.2 requires collection to be done by lawful and fair means, and not in an unreasonably intrusive way. Employers should therefore ensure that they collect the minimum amount of personal information necessary at the appropriate time, as collecting too much information too soon may be considered unreasonably intrusive. For example, applicants may be asked to provide additional personal information once they have been successfully selected for a position, such as banking details, a tax file number, and emergency contact details. However, this information should not be collected from all applicants at the time of submitting an application, if it is not necessary for the initial assessment of applicants’ suitability for a position.

Similarly, employers will usually ask applicants to provide details of nominated referees, in order to confirm their suitability for a position. However, to minimise the risk of unnecessary collection, referees’ personal information should be collected at an appropriate stage during the application process, such as after an interview and where an applicant has been shortlisted or selected for a position.

PROVIDING NOTICE OF COLLECTION TO APPLICANTS

Under IPP 1.3, VPS employers must take reasonable steps to tell applicants about certain matters regarding the collection of their personal information, such as the purposes for which the information is collected, and the main consequences (if any) if all or part of the personal information requested is not provided. This is usually referred to as a collection notice. Further information on collection notices is available on [OVIC’s website](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/).

Collection notices should be provided to applicants before or at the time of collecting their personal information, or if that is not practicable, then as soon as practicable after the collection. IPP 1 does not prescribe how notice must be provided, so it is up to the employer to decide the most appropriate way to provide a collection notice to applicants. For example, notice could be provided in writing in the initial job advertisement or on an application form, or verbally during an interview if additional personal information is being collected at that time.

Employers must take reasonable steps to provide notice to applicants for each new collection of personal information during the recruitment process, regardless of whether that same information has been collected previously. For example, an employer may provide a notice for personal information collected at the time an application is submitted, and then again when collecting the successful candidate’s banking details, even if some of the personal information collected in the latter instance is the same as in the first collection.

This requirement also applies throughout the course of an employee’s employment – if personal information is collected from employees at various times, reasonable steps to provide notice must be taken each time. This is particularly important if the personal information collected subsequently will be used for a different purpose than the original collection.

SHARING INFORMATION COLLECTED AS PART OF A REFERENCE CHECK

At the time of giving a reference, a nominated referee might request that the information they provide about an applicant remain confidential. However, employers should not guarantee confidentiality as applicants may request documents relating to the recruitment process, which may include information provided by referees during a referee check. Requests for access may be made to VPS employers through the *Freedom of Information Act* 1982 (Vic) (**FOI Act**) or under IPP 6, where applicable.

Regardless of the avenue through which the request is made, whether a request for access to documents relating to the recruitment process is granted will depend on the circumstances of each matter and should be determined on a case-by-case basis. For example, certain exemptions under the FOI Act or exceptions to IPP 6 may apply to restrict access to some or all of the information requested.

In every case, employers should be very clear about what information is being recorded and note that the applicant may request access to recruitment documents. This will enable the referee to understand what could potentially be released to an applicant, should they make a request for access.

CONTACTING SOMEONE WHO HAS NOT BEEN NOMINATED AS A REFEREE

An employer may wish to seek a reference from a person who has not been nominated by the applicant. For example, the applicant may not have nominated the most appropriate person to provide information about their suitability for a job (such as their current or most recent employer), or the nominated referee may not work closely enough with the applicant to give sufficiently detailed information.

If an employer decides that it is necessary to speak to an unlisted referee, they should always seek an applicant’s consent before doing so. Discussing this matter with the applicant provides them the opportunity to explain why they provided their chosen referees and did not list others. It also provides the employer with the opportunity to ensure adherence to IPP 1.5, which requires that notice of indirect collection be provided to individuals when personal information about them is collected from third parties.

SHARING PERSONAL INFORMATION ABOUT FORMER OR CURRENT EMPLOYEES TO PROSPECTIVE EMPLOYERS

In some cases, employers may be reluctant to share information about a current or former employee when asked to give a reference to a prospective employer. This may be due to, for example, uncertainty about whether the personal information can be lawfully disclosed, or what information is appropriate to share, particularly where it might relate to a delicate matter such as misconduct information.

When applying for a position, applicants should be encouraged to ensure they advise any nominated referees that they may be contacted to provide a reference, and that they (the applicant) consent to their personal information being shared. This permits the employer to disclose personal information about the applicant to a prospective employer under IPP 2.1(b).

Other exceptions under IPP 2 may also apply to permit personal information about a current or former employee to be shared with a prospective employer in the context of a referee check, such as where permitted or required by law (IPP 2.1(f)).

Employers may also wish to consider whether personal information relating to sensitive or delicate matters, such as employee misconduct, can be legally and appropriately disclosed as part of a referee check, and if relevant, noting this in an employee privacy policy or informing the individual to whom the information relates before the information is shared, in the interest of transparency.

BACKGROUND CHECKS

Under IPP 4.1, VPS employers are required to take reasonable steps to protect the personal information they hold – including employees’ personal information – from misuse, loss, and unauthorised access, modification or disclosure.

The reasonable steps taken by VPS employers should involve measures across different security areas: governance, information, personnel, ICT and physical security. One area that is particularly relevant to the recruitment process is personnel security, which involves ensuring only eligible and suitable people are engaged and employed and given access to information.

One personnel security measure that an employer may decide to adopt is pre-employment screening, to ensure prospective employees meet the organisation’s security requirements. Pre-employment screening may involve conducting different background checks, such as a police check or criminal record check. Background checks can be used to confirm the applicant’s eligibility or identity and to determine their suitability for the position.

In some instances, background checks (for example, Working with Children checks) may be required by legislation, depending on the nature of the role and the employer in question. In other cases, background checks may be conducted at the discretion of the employer.

Before requesting an applicant undergo a background check, the employer should first determine whether it is necessary for the position, or for the wider organisation’s security requirements. This can help to eliminate the unnecessary collection of personal information (including sensitive information) where an individual’s background history is not relevant to the performance of the job.

Employers should also ensure the type of check conducted is proportionate to the position, as some checks may require individuals to provide a substantial amount of sensitive and delicate information.

Further, background checks should only be conducted at an appropriate stage of the recruitment process – for example, once an applicant has been selected for the position.

ONLINE PROFILING DURING RECRUITMENT

Searching for information about an applicant on social media and other online sources and using that information to inform recruitment decisions is often known as online profiling. This practice can range from reviewing a blog, to a social media review, to conducting a systematic search to uncover every aspect of an individual’s online presence.

Employers who choose to search online for information about an applicant without their knowledge need to do so with caution, as there are a number of risks associated with relying on social media to screen potential employees. For example, information found online may not be accurate, complete or current, as content posted by an applicant may be out of date or no longer relevant, or third parties may post information about the applicant that is inaccurate or false. Online information may also not be available for all applicants.

If an applicant is not aware that online profiling will occur, they do not have the opportunity to correct potentially inaccurate or out of date information about themselves that could be used to inform the recruitment process. Additionally, online profiling carries the risk of over collection of personal information, including that of third parties. Employers can quickly lose control over the quantity and nature of personal information collected from online sources.

Online profiling may not always occur as part of a formal selection process; employers may conduct informal social media checks on applicants without actually collecting any personal information. However, even informal checks can carry a risk of introducing bias into the selection process and impacting a decision, regardless of whether this is done consciously or not. If accessing personal information about an applicant online – both informally and formally – organisations should ensure that they are transparent in their practices and record any instances of doing so.

MINIMISING THE PRIVACY RISKS OF ONLINE PROFILING

VPS employers who decide to conduct online profiling as part of a recruitment process should keep the IPPs in mind – in particular IPP 1. In this context, IPP 1 requires that only personal information necessary for the recruitment activity is collected, regardless of how or from where it is collected. Prior to conducting a social media search, employers should set clear parameters regarding what information they will collect to ensure they do not collect more information than is necessary for decision making, nor collect third party information.

IPPs 1.2 and 1.4 are also relevant in this context. IPP 1.2 requires VPS employers to collect personal information by lawful and fair means, and not in an unreasonably intrusive way – as such, employers should carefully consider whether the collection of personal information through online profiling aligns with this principle. Employers should also consider whether online profiling that results in the collection of personal information complies with IPP 1.4 which, if reasonable and practicable, requires personal information to be collected only from the individual whom the information is about.

Employers should also be transparent, and if online profiling is a standard practice for all applicants, they should advise individuals as such, for example in an application form. This will ensure potential applicants know to expect that profiling will occur, and provide them an opportunity to correct inaccurate or supplement incomplete information.

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice.