PRIVACY DURING EMPLOYMENT

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 the privacy obligations the owe to their employees.

PROTECTING EMPLOYEES’ PERSONAL INFORMATION

VPS employers are required to take reasonable steps to protect the personal information they hold (including of employees) from misuse and loss, and unauthorised access, modification or disclosure, in accordance with IPP 4.1.

Determining what is reasonable will depend on the context of each organisation, however as noted above, the measures that employers implement should cover all security areas: information, personnel, ICT and physical security, and governance.[[1]](#endnote-1) Some examples of security measures that employers can take to protect personal information are outlined below.

The Victorian Protective Data Security Framework (**VPDSF**) under Parts 4 and 5 of the PDP Act, which is the overall scheme for managing protective data security risks across the Victorian public sector, also applies to many VPS employers. The VPDSF includes the Victorian Protective Data Security Standards (**VPDSS**), which require organisations covered by Parts 4 and 5 of the PDP Act to adhere to a minimum set of protective data security requirements.[[2]](#endnote-2)

Restricted access

One information security measure that can be implemented to protect employees’ personal information is role-based access. Access to information about employees should be limited to those individuals who hold positions that are relevant to the handling of that information. For example, human resources management staff will require access to employee information for payroll purposes, however other staff members should not be able to see this information without a clear need to do so. Access may be restricted in a number of ways, including password protections for electronic data, locked cabinets for physical files, or swipe card access to restricted areas.

Protective Markings

Another information security measure that may be implemented to protect employees’ personal or sensitive information is a protective marking system. Protective markings indicate to individuals accessing the information the handling measures expected to be applied during the use, handling, storage, transfer and disposal of that information.

For example, applying a protective marking to emails or documents containing sensitive information about employees informs the level of protection that should be applied to that information.

DISCLOSING INFORMATION ABOUT EMPLOYEES

When disclosing an employee’s personal information, employers should ensure they have the appropriate legal authority to do so, under enabling or other legislation, or IPP 2.

Under IPP 2, VPS employers must not use or disclose employees’ personal information for purposes other than the original purpose of collection. However, IPP 2 contains eight exceptions that permit secondary use or disclosure, including where:

* the secondary purpose is related to the primary purpose of collection and the employee would reasonably expect their personal information to be used or disclosed for the secondary purpose (IPP 2.1(a));
* the use or disclosure is required or authorised by law (IPP 2.1(e));
* the employee has given their consent for the secondary use or disclosure (IPP 2.1(b)); or
* the employer reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to the life, safety or welfare of an individual or the public (IPP 2.1(d)).

Employers should communicate to employees what the organisation’s practices are for routine disclosures of personal information, as required by IPP 1.3, and in the interest of openness (IPP 5). This can be done through a privacy policy, and through a collection notice provided when collecting personal information.

Investigating suspected unlawful activity

Where an employer has reason to suspect that unlawful activity has been, is being, or may be engaged in, IPP 2.1(e) may allow an employee’s personal information to be used or disclosed:

* as a necessary part of the employer’s investigation of the matter; or
* in reporting the employer’s concerns to relevant persons or authorities.

Where an employer proposes to use or disclose personal information in order to investigate a matter itself, any suspicion of wrongdoing should be based on reasonable grounds, and the use or disclosure must be considered necessary after due consideration of alternatives.

If an employer decides to report suspected unlawful activity by an employee, it should be done only to those organisations that need to know the information in order to carry out the necessary investigation(s). Employees should be informed that their information may be used or disclosed for these reasons, for example in the organisation’s privacy policy.

Complaint handling

Employees may complain to their employers about a range of issues, including sensitive matters such as bullying in the workplace. Some considerations for VPS employers to keep in mind when collecting, using and disclosing employees’ personal information in the context of a complaint include:

* Anonymity: IPP 8 states that where lawful and practicable, individuals must have the option of not identifying themselves when entering into transactions with an organisation. Depending on the nature of the complaint, it may be possible or appropriate for employees to make complaints anonymously.

However, in other cases an employer may need to collect personal information about the employee making the complaint, and subsequently use or disclose that information, in order to investigate, handle, and resolve the complaint.

* Disclosure: some complaints may require the disclosure of personal information of the employee making the complaint – for example, to a colleague who may be the subject of the complaint, in order to afford that individual natural justice and give them a right of response as part of investigating the complaint; or to a different part of the organisation or an external body that is more appropriate to deal with the complaint.

Regardless of who personal information is disclosed to, the disclosure must be permitted under IPP 2, whether for the primary purpose of collecting the information, or a permitted secondary purpose such as those listed above. If relying on IPP 2.1(a), employers will need to consider whether the proposed disclosure would be reasonably expected by the complainant.

Employers should also avoid excessive disclosures of personal information, and only share what is necessary for the purposes of handling and resolving the complaint.[[3]](#endnote-3)

* Public interest disclosures: Where an employee makes a complaint that relates to public sector corruption or police misconduct, it may need to be referred to the Victorian Independent Broad-based Anti-corruption Commission (IBAC). In some circumstances, the complaint may become a public interest disclosure, which provides legal protections under the Public Interest Disclosures Act 2012 (Vic) to individuals reporting improper conduct and corruption.

Heads of departments, Council CEOs and other relevant Principal Officers also have mandatory reporting obligations, which require them to notify IBAC of any matter where it is suspected, on reasonable grounds, that corrupt conduct has occurred or is occurring.[[4]](#endnote-4)

EMPLOYEE MONITORING AND SURVEILLANCE

Employers may conduct monitoring and surveillance of employees for a number of reasons. Whatever the purpose, these activities will likely involve collecting personal information about employees, or information which may reveal the identities of employees. There are many different types of technologies that can be used for the surveillance and monitoring of employees, both within and outside of the workplace. Some methods and technologies, and key considerations for VPS employers, are outlined below.

Regardless of the technology or device used, employers planning to conduct employee surveillance and monitoring should seek legal advice regarding their obligations under the SD Act and other relevant legislation. Employers must also ensure that any monitoring and surveillance of employees is authorised under the PDP Act, or other enabling legislation.

Conducting a PIA before implementing a surveillance or monitoring program is crucial to identifying any privacy impacts and risks associated with the proposed practice.

Monitoring email, phone and internet use

An employer may decide it is necessary for its functions and activities to monitor employees’ email, phone or internet use. For example, it may be necessary for an employer to:

* have access to an employee’s work emails when the employee is absent for an extended period of time, or for security reasons;
* monitor employees’ internet use to ensure appropriate use, or to track any viruses or malware that threaten systems or networks; or
* listen to or record work-related telephone calls for quality and assurance purposes, or for training other staff.

Monitoring activities involving the collection of personal information that is not necessary for an employer’s functions or activities would contravene IPP 1.1, or could be considered unreasonably intrusive or unfair under IPP 1.2 if done covertly where there is no legal basis for doing so.[[5]](#endnote-5)

Clear communication between employers and staff about what monitoring practices are in place within the organisation, under what circumstances staff may be monitored, and for what purposes they will use any information collected will help mitigate the risk of complaints and prevent an erosion of trust between employer and employee, and satisfy the notice requirements of IPP 1.3.

Employers may wish to develop an appropriate use policy so that employees are aware of how they are expected to use business tools such as emails or internet access. For example, if personal calls are not to be made during business hours, the policy should clearly state this.

GPS tracking

Technology provides more and more opportunities for employers to track the movements of their employees. For example, GPS tracking in vehicles enables employers to monitor the movements of employees travelling in company cars, and location services in work mobile phones can pinpoint an employee’s location. Some employers may decide it is necessary to track and collect information about the movements of their employees. Whether or not the use of these technologies is reasonable or intrusive will depend on the purpose for which the information is used, and how it is tied to the organisation’s functions or activities.

Employees should be notified when GPS tracking will occur (such as whether it is only during business hours or also includes out of office hours), what information is being collected and why, what it will be used for, and the consequences if employees object to being tracked.

Where there is no legitimate purpose for tracking employees, employers should make sure that GPS tracking is disabled where possible before issuing a device with this capability to employees.

Surveillance cameras

CCTV cameras are often used as a security measure (for example to enhance safety or deter crime), or to monitor employees or the activities within a workplace during business hours.

As the use of surveillance cameras will likely involve the collection of personal and potentially sensitive information (for example, images or footage of identifiable individuals), employers should be able to identify a legitimate purpose for the surveillance, and only collect personal information via the cameras if the information is necessary for the employer’s functions or activities, in accordance with IPP 1.

Where employers identify a legitimate purpose for surveillance or monitoring, they should ensure that the use of cameras is proportionate to achieving that objective – surveillance cameras should not be used simply because they are cost effective or convenient. There may be other equally effective but less intrusive means to achieve the organisation’s objective.

Where personal and potentially sensitive information is collected through CCTV cameras, employers must ensure they handle the captured information in accordance with the IPPs. For example, employers must notify employees that they could be under surveillance while in the workplace, and employees should be provided with details of their employer’s practices based on the matters set out in IPP 1.3.

In some cases, it may be appropriate to layer the collection notice by displaying signage advising employees and visitors that they may be under surveillance, and including a link to the relevant surveillance or privacy policy. As with any personal information, employers must ensure that the personal information captured via surveillance cameras is used only for the purposes for which it was collected, unless an exception applies.[[6]](#endnote-6)

Data analytics

The use of data analytics is growing across all areas of government, including for the purposes of monitoring employees. For example, some organisations use data analytics as a fraud and corruption prevention strategy to combat conflict of interest risks, by examining large amounts of data from various sources to identify outliers, correlations and patterns.

For example, the use of data analytics in this context may involve matching employees’ information (such as payroll and contact details) against supplier data or conflict of interest declarations, to manage fraud and corruption risks in procurement processes.

As with other methods of monitoring, employers must ensure that there is a legitimate purpose for the data matching, and its use is proportionate to achieving that purpose. Employers must also ensure that the use of employees’ personal information in data matching activities is permitted under IPP 2 – for example, personal information such as bank account details are generally collected for payroll purposes, and its use in data matching would therefore likely constitute a secondary use. This secondary use must be permitted under an exception under IPP 2.

IPP 5 is another consideration. As noted above, being transparent about monitoring activities is crucial to help maintain trust between employers and employees, and ensure that employees are aware of the range of purposes to which their personal information may be put, including for monitoring through analytics.

Employers undertaking or looking to commence data analytics for monitoring purposes must also consider the remaining IPPs – for example, personal information must be accurate, complete and up to date before being used in data matching activities in line with IPP 3; and any personal information generated or inferred as a result of such activities must be adequately protected, and disposed of once no longer needed for any purpose, in line with IPP 4.1 and 4.2 respectively.

DRUG AND ALCOHOL TESTING

In some workplaces, employers may test employees for drugs or alcohol. Such tests may be necessary for the organisation’s functions and activities – for example, if an employee is required to operate a vehicle or heavy machinery, having drugs or alcohol in their system could pose a serious safety risk. However, where such testing is not relevant or required for the specific role, the collection of employees’ information from these tests may be considered unreasonably intrusive or unfair.

As with other personal information collected from or about employees, the IPPs will apply to personal information collected during drug or alcohol testing. IPPs 1 and 2 are particularly relevant in this context – for example, employers must ensure employees are aware of the matters listed in IPP 1.3, particularly the purposes for which the information will be used, and the consequences for employees if they refuse to take the test. In accordance with IPP 2, employers should not use or disclose personal information obtained from the tests for purposes other than the original purpose for collection, unless authorised under the PDP Act or other legislation.

VPS employers should note that the results of a drug or alcohol test may be classed as health information. As such, employers should check their obligations under the HR Act where health information may be collected via such tests. Before implementing drug and alcohol testing programs, employers should complete a PIA to avoid the potential over collection of personal information and identify any privacy risks that may arise from the practice.

‘BRING YOUR OWN DEVICE’ PROGRAMS

‘Bring your own device,’ or BYOD, is an arrangement that enables employees to use personal devices for both personal and business purposes. While there are benefits to BYOD programs, there can be significant privacy and data security risks for both the corporate information and the personal information contained on a device, if inadequate procedures and controls are in place. For example, as it expands the number of networks, applications, and end points through which an organisation’s data may be accessed, BYOD can increase the vulnerabilities in an organisation’s ICT system and threaten its information assets, including personal information holdings.

Before implementing a BYOD program, employers should conduct both a PIA and a security risk assessment to ensure that the measures put in place to protect official information (including personal information) are commensurate with the potential impact if the information were compromised.

Organisations with a BYOD program should also have specific BYOD policies, including terms of use for employees to follow. For example, it might be a condition of use that employees protect their devices with a password, and that they offer their devices to their organisation’s ICT professionals to configure the appropriate security settings.

While it is important to ensure the security of business information, the privacy of personal information of those employees participating in a BYOD program should be considered, particularly given that many individuals’ personal lives are entwined with their mobile devices.

 A clear BYOD policy that outlines what personal information an organisation can collect from the device, and in what circumstances, will help to protect employees’ privacy and promote trust between the employer and its employees.

Work devices used for personal use

In contrast to BYOD, employees may be provided with a work-issued device, which may then also be used by an employee for personal purposes. This could potentially result in the employer collecting personal information about the employee that is contained in the device, for example during a backup of the device. The collection of any personal information would then attract obligations under IPP 1 and the other IPPs, including, potentially, notice requirements.[[7]](#endnote-7)

As with BYOD, employees should be provided with any policies or terms of use relating to the use of work devices for personal use. If there is potential for an employer to collect personal information from work devices, such collection should be authorised and the IPPs applied to any personal information collected.

BIOMETRIC SYSTEMS

Some workplaces may use biometric systems for a variety of purposes, such as verifying employees’ identities to enable access to a building or office. While biometrics may offer benefits, employers should be aware of the limitations and privacy risks arising from the use of biometrics in the workplace – for example, function creep (employees’ biometric information is used for a different purpose than the original purpose of collection), or the potential for biometric information to reveal secondary information about an employee.

While the definition of sensitive information under the PDP Act does not include biometric information (unlike the Commonwealth *Privacy Act 1988*), some biometric characteristics may reveal sensitive information as defined under the PDP Act, the collection of which may breach IPP 10. Given the inherently personal nature of biometric information, employers should consider treating such information they collect as delicate, and be cautious with how this information is handled. For more information about biometrics and the interaction with the IPPs, see OVIC’s resource on [*Biometrics and privacy*](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/)*.*

WORKING REMOTELY

VPS employers may allow employees to work remotely, such as from home, on an ad hoc or regular basis, or as needed in certain circumstances (for example, where doing so is part of an organisation’s business continuity plan).

A remote work environment can present unique information and cyber security risks, so employees need to ensure they take appropriate steps to protect any public sector and personal information they access when working remotely, and continue to uphold their privacy obligations under the PDP Act and other applicable legislation.

Organisations should ensure that employees are also aware of any relevant workplace policies that may apply, and promote good privacy and security practices for working remotely. For useful tips see OVIC’s resource [*Tips for working remotely and protecting privacy*](https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/).

END OF EMPLOYMENT

The IPPs apply to all personal information collected and held by VPS employers regardless of the employment status of the individual involved. Employers therefore continue to have responsibilities to protect an individual’s personal information at the end of their employment, and after they have left the organisation.

Retention of employees’ personal information

IPP 4.2 requires VPS employers to take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose. An organisation’s enabling legislation, or other relevant legislation such as the *Public Records Act 1973* (**PR Act**), may contain requirements in relation to the retention of personal information, including of employees specifically. VPS employers must retain relevant personal information of employees in accordance with any applicable retention and disposal requirements issued by the [Public Record Office Victoria](http://prov.vic.gov.au/).

Beyond this, an employer may only keep the personal information of its former employees where it can identify a relevant purpose for doing so; for example, where it is required by law or as part of an ongoing investigation.

1. For more information about ‘reasonable steps’, see the IPP 4 chapter of the *Guidelines to the Information Privacy Principles* at <https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/>. [↑](#endnote-ref-1)
2. More information about the VPDSF and VPDSS is available at <https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/>. [↑](#endnote-ref-2)
3. For examples of ‘reasonably expected’ and ‘excessive disclosure’ in the context of complaints, see Case Studies 2F, 2G, 2I, 2J and 2K in the IPP 2 chapter of the *Guidelines to the Information Privacy Principles*, at <https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/>. [↑](#endnote-ref-3)
4. For more information about public interest disclosures and mandatory notifications, see IBAC’s website at <https://www.ibac.vic.gov.au/reporting-corruption>. [↑](#endnote-ref-4)
5. For information about privacy risks associated with monitoring employees’ social media accounts, see OVIC’s *Social Media and Privacy* resource available at <https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/>. [↑](#endnote-ref-5)
6. For guidance on surveillance best practice, see OVIC’s resource on *Surveillance and privacy in the Victorian public sector*, available at <https://ovic.vic.gov.au/privacy/privacy-guidance-for-organisations/>. [↑](#endnote-ref-6)
7. The PDP does not distinguish between solicited and unsolicited collection of personal information. The IPPs therefore apply to personal information regardless of whether it was solicited or unsolicited by an organisation.

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice. [↑](#endnote-ref-7)