Office of the Victorian Information Commissioner

INFORMATION FOR REGULATED ENTITIES

Smart glasses and other smart wearable technologies

Privacy, information security and public access considerations

The Office of the Victorian Information Commissioner (**OVIC**) is Victoria's primary integrity agency and source of independent advice about how the Victorian public sector collects, uses and discloses information.

This guidance is for organisations subject to the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) and *Freedom of Information Act 1982* (Vic) (**FOI Act**). This includes Victorian government departments, Ministers, local councils, statutory offices, government schools, universities, and TAFEs. OVIC does not regulate the actions of members of the public, the private sector, or public sector organisations operating in other Australian jurisdictions.

This guidance relates to obligations under the PDP Act and FOI Act. Other legislation, including the *Surveillance Devices Act 1999* (Vic) (**Surveillance Devices Act**), may govern the collection of information through smart wearable technologies and the further use and disclosure of that information. OVIC does not administer the Surveillance Devices Act.

What are smart wearables?

Smart wearables are everyday consumer items with built-in digital technology such as speakers, microphones, cameras and an Artificial Intelligence (**AI**) assistant that usually connect wirelessly to the user's smartphone. The AI assistant uses data collected through the smart wearable to analyse the user's surroundings and provide data to the user, such as translations, transcripts and summaries of conversations, object recognition, internet search results and recommendations. Capabilities differ, depending on the make and model. Examples of smart wearables include smart glasses, smart watches and smart pendants. Other smart wearables may soon become available, such as earbuds with built-in cameras that enable AI assistants to analyse the wearers surroundings.

Smart glasses and other wearables can be useful hands-free accessibility tools for people with vision, hearing, mobility or cognitive impairments.

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

As smart wearables become more affordable and available to consumers, organisations should expect an increase in staff, stakeholders and members of the public using smart wearables in government workplaces and government-run facilities.

Main privacy concerns

The main privacy concerns arise from smart wearables that have discreet built-in camera, video or audio-recording capability that is continuously on or can be switched on and off by the user. Due to their discreet design, people within line-of-sight or audio range, may not know that the camera or microphone is turned on, and therefore may be unaware that their image is being captured or their conversations or actions are being recorded, analysed and made available to the wearer for future use.

Smart wearables can be contrasted with smartphones. When a person uses their smartphone to take a picture in a public, semi-public or intimate space, the action is more obvious to those around them and people can exercise some choice about what to do. They can move out of the camera frame, ask the person to stop taking photos or video or report the behaviour. Smartphones are also not designed to continuously record audio, and we do not generally expect other people to be recording us as we move about our day.

Smart wearables are different. Their discreet design and focus on the collection and analysis of environmental data makes it difficult for people to make privacy choices, and challenges social norms around appropriate and inappropriate recording of others.

In future, smart wearables with cameras may be capable of continuously taking photos every few seconds throughout the day, or may be integrated with facial recognition technology, creating significantly higher privacy risks for people in the wearer's surroundings.

Privacy obligations

Where an organisation uses smart wearable technology for authorised work purposes, the collection and handling of personal information must comply with the Information Privacy Principles (**IPPs**) in the PDP Act.

Under IPP 1, the collection must be necessary, lawful, transparent and fair:

- **Necessary:** An organisation should not collect more personal information than it needs, where more privacy preserving options are reasonably available.
- **Lawful:** The collection needs to be lawful under criminal and civil law, statute and common law.
- **Transparent**: Individuals should be told about the collection of their information before, or at the time collection occurs.

- **Fair**: Discreet or covert collection through smart wearables is likely to be unfair. It may also be unreasonably intrusive, depending on the intimacy of the setting and the availability of less intrusive methods of collection.

Where the purpose of using the camera or audio recording is to collect and use **sensitive information**, organisations must comply with IPP 10. This means the collection should only occur where individuals have provided their **consent**, unless one of the other limited circumstances in IPP 10 applies.

Main information security concerns

The discreet design of smart wearables with built-in cameras or microphones creates information security risks for organisations. Personnel or visitors may be wearing smart glasses, smart watches, smart pendants or other smart wearables while attending workplace facilities and accessing workplace environments, systems and information. If the camera or microphone in the smart wearable is turned on, the individual can make a record of what they see or hear. This record may be disclosed to others, including the company that operates the smart wearable or its AI assistant, and data may be processed outside Australia, without prior approval from your organisation. The presence of smart wearables in workplace settings presents higher security risks where the wearer has access to information that may be considered sensitive or significant (for example, PINs, usernames and passwords, financial data or personal and health information of employees and members of the public).

Information security obligations

- The Victorian Protective Data Security Standards (**VPDSS**) in Part 4 of the PDP Act require regulated organisations to, amongst other things, manage information security risks, control access to public sector information, implement and maintain ICT security and physical security controls, ensure all persons understand their responsibilities to protect public sector information, and ensure third parties handle public sector information securely. Part 4 of the PDP Act requires organisation heads to ensure that their organisation and its contracted service providers comply with VPDSS requirements.

- IPP 4 requires organisations to take reasonable steps to protect the personal information it holds from misuse, and from unauthorised access, modification or disclosure. Organisations must anticipate foreseeable security risks to the personal information they hold and take reasonable precautions to protect the information from those risks. Organisations must also destroy or de-identify personal information when it is no longer needed, in line with recordkeeping obligations in the *Public Records Act 1973* (Vic).

What should organisations do?

- All organisations should consider the information security risks that smart wearable technologies may pose in a workplace context, including the physical environment and information and systems that personnel and visitors can access. A security risk assessment will assist organisations in identifying information security risks associated with smart wearables and the mitigations required to reduce risks to an acceptable level.

- Organisations that currently restrict photography and recording in certain settings, should consider whether signage and policies need updating, to ensure it is clear to individuals that the restriction applies not only to the use of mobile phones, but to the use of camera and recording capability in any device or wearable technology.

- Organisations may need to review and update organisational policies, to ensure that the use of smart wearable technologies by employees, contractors and volunteers is appropriately addressed. When updating policies, organisations should consider the use of smart wearables in improving accessibility for persons seeking reasonable adjustments across the employee lifecycle. Policies may relate to ICT use, information security, privacy, inappropriate access to personal information, fraud and corruption, bring your own device, records management and incident management. Updated policies and procedures should be made visible to all employees, contractors and volunteers.

- Organisations considering authorising the use of a smart wearable technology, should conduct a privacy impact assessment and security risk assessment of the specific wearable's capabilities, the wearer's role and level of access, and purposes of use, to ensure the technology is used appropriately, and privacy and security risks are identified and mitigated. The improved accessibility that smart wearables can provide for persons seeking reasonable adjustments across the employee lifecycle should be considered when assessing risks and identifying mitigations.

- Information captured via smart wearable technology for authorised work purposes may be in the possession of the organisation and able to be requested by an applicant under the FOI Act. Organisations should ensure information collected or generated by smart wearables is properly captured and stored in approved electronic document and records management systems, to give proper effect to the right of access and correction under the FOI Act, and where applicable, IPP 6. To maintain public trust, organisations should proactively explain to the public their use of smart wearable technologies.

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

OVIC resources

- IPP Guidelines:
    - IPP 1 – Collection
    - IPP 10 – Sensitive Information
    - IPP 4 – Data security
    - IPP 9 – Transborder data flows
- Privacy Impact Assessment guide and template
- Victorian Protective Data Security Standards
- Assessing the security value of public sector information
- Business Impact Level table
- Conducting a security risk assessment
- FOI Guidelines - Document of an agency
- Proactive release

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