Office of the Victorian Information Commissioner

INFORMATION FOR THE PUBLIC

Unpacking your right to privacy

How is privacy protected in Victoria?

In Victoria, you have information privacy rights under the *Privacy and Data Protection Act 2014* (Vic)(**PDP Act**).

The PDP Act contains 10 Information Privacy Principles (**IPPs**) that Victorian public sector (**VPS**) organisations must comply with. These principles provide a consistent framework for VPS organisations to interpret and apply when carrying out their work to ensure that the handling of your personal information is lawful.

Tips for exercising your privacy rights

You can exercise your privacy rights by:

- reading the notice of collection provided to you when asked for your personal information
- refusing to provide information that the organisation indicates is 'optional' on a form
- asking questions about why your information is needed before you provide it if you have concerns, or do not understand why your information is being collected
- making a privacy complaint to a VPS organisation's privacy officer. If you cannot resolve it with the organisation, you can then escalate the complaint to OVIC.

Common misconceptions

- There's no definitive list of what is, or isn't, an interference with your privacy – it will depend on the circumstances.
- VPS organisations don't always need your consent to collect, use, or disclose your personal information.

- After a data breach, an organisation may request you delete or destroy the information you received by mistake. This is not an attempt to 'cover up' the incident, rather – it is a best practice step OVIC encourages organisations to take to contain the spread of information, and protect individuals from further harm.

- Not all privacy complaints warrant financial compensation, even if an organisation has conceded it has interfered with your privacy.

What to do if you've been impacted by a data breach

If you have been notified by a VPS organisation that your personal information has been involved in a data breach, you should read our guidance on how you can reduce the risk of harm to you as a result of the breach.

What to do if you receive, or find, information meant for someone else

On rare occasion, you may receive, or find, information that is not meant for you.

Incidents like this can happen where an email is accidently sent to the wrong recipient, or a VPS employee has dropped a USB device, left their laptop or a notebook on a train, or documents are found on the ground.

If you receive, or find, information meant for someone else:

You should:

1. Urgently identify the VPS organisation the information belongs to, and contact them to inform them of the error – this should trigger the organisations data breach response process.

    - You can identify the organisation by looking for its name, logo or branding at the top or bottom of a page, or the email address the information was sent from.

2. Follow the instructions provided by the organisation to destroy, or return, the information you have received or found.

You should not:

- Open a letter addressed to someone else, you should instead return it to the sender

- Take photos of the information and share it with others, or post it on social media

- Contact any individuals identified within the information, this is likely to cause more harm than good.