Minimising the privacy impacts of an incident

The Office of the Victorian Information Commissioner and Public Record Office Victoria have issued a joint statement regarding how Victorian public sector organisations can minimise the privacy impacts of an incident

The Office of the Victorian Information Commissioner (**OVIC**) and the Public Record Office Victoria (**PROV**) have produced this joint statement as a resource for public sector organisations (organisations) to use as a basis for the necessary measures that protect the personal information they hold.

Organisations, and the information they hold, are increasingly at risk of data breaches. These impacts can be minimised by being prepared.

Although organisations can experience incidents involving any type of public sector information, this statement focuses on incidents involving personal information.

An incident can be caused by many factors, including malicious acts by an external or internal party, human error, or by a failure of an organisation to implement effective information management or security practices.

Incidents can result in organisational reputational damage, disruption of services, financial loss and loss of public trust in organisations. In some cases, incidents can also cause significant harm to the individuals whose personal information was involved. Individuals affected by incidents may experience embarrassment, emotional distress, physical harm, identity theft and fraud.

Minimum expectations for organisations

Organisations must look at their information management practices holistically when protecting the personal information they hold. Information privacy, information security and recordkeeping practices are all relevant to minimising the privacy impacts of an incident.

OVIC and PROV have set out their minimum expectations below, outlining the steps organisations should take to minimise the privacy impacts of an incident.

1. **Do not collect more personal information than is necessary for functions or activities.** Over-collection of personal information may lead to more information being compromised in a data breach, resulting in more adverse consequences for the individuals whose personal information was involved. Organisations must create and keep full and accurate records of their decisions and actions. However, records must not include more personal information than necessary.

2. **Implement strong information security practices in line with organisational obligations.** Strong information security practices should be in place to protect personal information (and all other forms of public sector information) from misuse, loss, and unauthorised access, modification or disclosure. Information security practices must be regularly reviewed and updated as required. Organisations covered by Part 4 of the *Privacy and Data Protection Act 2014* (**PDP Act**) must adhere to the Victorian Protective Data Security Standards (**VPDSS**).

3. **Have a records disposal program in place.** Personal information is at greater risk of being involved in an incident when records are held for longer than the required minimum legal retention period (as specified in PROV Retention and Disposal Authorities issued by the Keeper of Public Records). An effective disposal program for records held – in all formats and within all systems and storage environments – is a critical component of protecting personal information.

4. **Do not de-identify records before the minimum retention period is reached.** Once created for official purposes, records should not be de-identified before the minimum retention period is reached, to ensure the records retain their value for their original purpose. Permanent value records must not be de-identified. Transferring permanent value records to PROV at the appropriate time will assist in preserving and protecting that information.

5. **Consider the risks involved with de-identification.** De-identifying records containing personal information and continuing to hold them past the required minimum legal retention period is risky, as data re-identification tools and methods become more sophisticated.

6. **Build protections into third-party arrangements.** Outsourcing government business to third parties can place records that contain personal information at risk. It is critical that third-party arrangements (such as contracts) specify requirements for creating, managing, storing, protecting and disposing of records, and that these arrangements are regularly reviewed.[1] Third parties must comply with the arrangements and dispose of government information within a required period. If subcontracting work, the third-party provider must ensure that the subcontractor complies with the requirements and organisations are aware of any subcontracting arrangements

[1] Organisations covered by Part 4 of the PDP Act have a legislative obligation to ensure a contracted service provider does not do an act or engage in a practice that contravenes the VPDSS in relation to public sector information collected, held, used, managed, disclosed, or transferred by the provider for the organisation. See section 17 of the PDP Act for how the Information Privacy Principles apply to third party arrangements.

7. **Develop an incident response plan.** An incident response plan should be in place to set out how organisations will:

    - respond in the event an incident occurs
    - establish a core incident response team
    - involve the organisation's lead privacy officer and records manager
    - detail post incident activities
    - test the plan, regularly, to make sure it is adequate.

8. **Train staff to act when they identify an incident.** Organisations should provide training to all staff and contracted service providers on what to do, and who to tell, if they identify a potential incident.

9. **Notify OVIC.** If organisations experience an incident involving personal information, they are encouraged to notify OVIC. OVIC can assist organisations in managing the breach. Organisations that are subject to the VPDSS must notify OVIC of certain information security incidents (some of which may involve personal information). Organisations must also report cyber incidents to the Victorian Government Cyber Incident Response Service.

OVIC and PROV can assist organisations in understanding their obligations to protect the personal information they hold and manage their records appropriately. Contact OVIC at enquiries@ovic.vic.gov.au and contact PROV at agency.queries@prov.vic.gov.au

Support resources

Managing the privacy impacts of a data breach: https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/

OVIC information Security Incident Notification Scheme: https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/

Information security and privacy incident notification form: https://ovic.vic.gov.au/privacy/resources-for-organisations/information-security-and-privacy-incident-notification-form/

Victorian Cyber Incident Response Service: https://www.vic.gov.au/report-or-respond-cyber-incident

Guidelines to the Information Privacy Principles: https://ovic.vic.gov.au/privacy/resources-for-organisations/guidelines-to-the-information-privacy-principles/

Victorian Protective Data Security Standards: https://ovic.vic.gov.au/information-security/standards/

An introduction to de-identification: https://ovic.vic.gov.au/privacy/resources-for-organisations/an-introduction-to-de-identification/

The limitations of de-identification – Protecting unit-record level personal information: https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/

PROV Recordkeeping Standards Framework: https://prov.vic.gov.au/recordkeeping-government/standards-framework

PROV Retention and Disposal Authorities: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept/retention-and-disposal-authorities-rdas

PROV guidance on managing privacy and recordkeeping obligations: https://prov.vic.gov.au/recordkeeping-government/a-z-topics/privacy-and-recordkeeping-obligations

PROV guidance on disposing of records: https://prov.vic.gov.au/recordkeeping-government/how-long-should-records-be-kept