

WA PRIVACY LAWS: WHAT LOCAL GOVERNMENTS NEED TO DO NOW.

Western Australia's new privacy laws now apply to local governments, introducing new requirements for how personal information is collected, used, shared, stored and managed. Local governments should review their privacy governance, policies, complaint processes, information-sharing practices and third-party arrangements to ensure they comply with the new framework.

With serious data-breach reporting requirements commencing on **1 January 2027**, local governments should also ensure they have clear incident-response procedures, appropriate internal responsibilities and processes for responding to and reporting serious data breaches.

WHAT DO WESTERN AUSTRALIA'S NEW PRIVACY LAWS REQUIRE LOCAL GOVERNMENTS TO DO, AND HOW SHOULD LOCAL GOVERNMENTS PREPARE FOR SERIOUS DATA-BREACH REPORTING FROM JANUARY 2027?

Western Australia's privacy and information-sharing laws took effect on 1 July 2026 and apply to local governments. Public entities must now manage personal information in line with the new framework, including its privacy principles, while preparing for serious data-breach reporting from 1 January 2027. This article outlines the practical priorities for governance, records, customer service, digital and people teams.

PRIVACY OBLIGATIONS NOW APPLY TO LOCAL GOVERNMENTS

The Privacy and Responsible Information Sharing Act 2024 (WA) (the PRIS Act) established a new framework for the handling of personal information by Western Australian public entities. Its privacy and data-sharing provisions came into force on 1 July 2026, and local governments are among the entities required to comply.

The framework is overseen by the Information Commissioner in relation to privacy and by the Chief Data Officer in relation to responsible information sharing. It sits alongside, rather than replaces, existing Freedom of Information Act 1992 responsibilities.

For local governments, the changes extend beyond information technology. Personal information is collected and used across rates, planning, libraries, recreation, community programmes, customer requests, human resources, CCTV and online services.

WHAT ARE THE CORE OBLIGATIONS?

The PRIS Act introduces Information Privacy Principles (IPPs) governing how personal information is collected, used, disclosed, stored and disposed of. The appropriate response to the handling of that data will depend on each local governments' functions and systems, but the following areas warrant immediate attention.

- Privacy governance: appoint and support a privacy officer at an appropriate senior level, with clear responsibilities and escalation pathways.
- Privacy policy and collection notices: ensure public-facing notices and policies accurately explain what information is collected, why it is needed, how it will be used and when it may be shared.
- Public registers: review access and secondary-use controls for registers administered by the local government.
- Privacy impact assessments: establish a process for assessing new or changed activities that may have a high privacy impact before they proceed.
- Contracts and suppliers: review service-provider arrangements where third parties collect, host or use personal information for the local government.
- Records and security: confirm that records-management, access-control and retention practices support the privacy principles.

It is also important to note that while the substantive provisions of the PRIS Act, including the IPPs commenced on 1 July 2026, some IPPs will apply to personal information that was collected before 1 July 2026.

A NEW PATHWAY FOR PRIVACY COMPLAINTS

Individuals may raise a privacy complaint with the relevant local government about an alleged interference with privacy. A complaint will generally need to be made to the local government first before it can be taken to the Information Commissioner.

Local Governments should therefore have a documented privacy-complaint process, clear ownership for investigations and a consistent approach to communicating with complainants. Existing complaint-handling processes may need adjustment so privacy matters can be identified, recorded and resolved appropriately.

RESPONSIBLE INFORMATION SHARING REQUIRES CLEAR DECISIONS

The new regime also provides a framework for government information sharing. It is intended to enable appropriate sharing where there is a permitted purpose and the relevant principles, safeguards and decision-making requirements are met.

Local Governments should not assume that a useful purpose alone is enough to share personal information. Proposed sharing arrangements should be assessed against the legislative framework, with appropriate records kept of the decision and safeguards applied.

THE NEXT DEADLINE: SERIOUS DATA-BREACH REPORTING

From 1 January 2027, agencies must begin reporting serious data breaches. This gives local governments a limited period to test incident-response arrangements, confirm internal responsibilities and ensure that legal, communications and technology teams can work together quickly if an incident occurs.

Preparation should include a current data map, a clear escalation process, an incident-response plan and exercises that test how the local government would assess a suspected breach and communicate with affected people and the Information Commissioner.

PRACTICAL PRIORITIES FOR LOCAL GOVERNMENTS

The new laws are now part of the operating environment for every Western Australian local government. A proportionate implementation plan should identify the highest-risk information practices, allocate accountable owners and establish a programme of review and training.

The immediate focus should be on privacy governance, policies, collection practices, public registers, high-risk projects and third-party arrangements. Local government should also use the period before January 2027 to strengthen their capacity to respond to a serious data breach.

The information provided in this article serves as a general guide and does not constitute legal advice. It is based on our research and experience at the time of publication. **Please consult our knowledgeable legal team** for any specific inquiries or advice relevant to your circumstances, as the content may not have been updated subsequently.