



yorb | DATA GOVERNANCE JOURNEY

The Privacy Act 2020, Anti-Money Laundering legislation (AML), General Data Protection Regulation (GDPR) are local and international laws that have impact the way we store and use data. The correct controls need to be put in place to prevent external access, but also unauthorised internal access. Microsoft 365 provides tools that:

- Enables data to be classified, increasing security, and improving search.
- Prevents accidental access to or distribution of sensitive materials.
- Prevents sensitive data from being, saved, shared, copied, printed or modified by unauthorised persons.
- Improves searchability of your data, ensuring your team can find what they need, when they need it.

01

DATA ASSESSMENT

Know where you are... Gaining an understanding of the current state and scale of any potential future work should be your first step.

- Where is your data stored?
- Do any existing policies exist to protect your data?
- Are you storing any sensitive data that requires additional controls?

02

POLICIES / GOVERNANCE

Know where you are going...

- Do you have documented data management policies? What is acceptable use of data, who should have access?
- Ensure you have documented data management standards.

Consider the type of data you keep, where it should be kept, and how long it should be kept.

03

DATA RESTRUCTURE

Is your data in a logical state?

Having a sound structure is critical to ensuring future work is successful.

04

DATA LEAK PREVENTION & INFORMATION RIGHTS MANAGEMENT

Put in place systems to ensure sensitive data is managed appropriately. Ensure Data Leak Prevention is enabled to minimise the chance of accidentally data loss.

Note: Someone intentionally trying to steal data will get around Data Leak Prevention. DLP is to prevent accidental loss (with the current BP license).

Ensure all documents are tagged with the appropriate sensitivity labels upon creation. This helps ensure your most sensitive data has additional controls to keep it safe, including encryption, auditing and tracing.

05

DATA LIFECYCLE MANAGEMENT

Similar to data sensitivity labels, labels can be applied to data upon creation that enable data lifecycle controls to be applied. This helps ensure obsolete data is removed from the system. Ensure:

- Data is retained as appropriate to your Data Governance policy.
- Audit logging exists to manage any behaviour that deviates from your lifecycle.
- Create automated controls that enable specific behaviour such as deletion or archival at the conclusion the tagged lifecycle.

06

TAXONOMY / METATAGS

Tagging your data upon creation with a well-designed data taxonomy enables:

- More relevant search results.
- Faster and more focussed access to data when you need it.
- Increased ability to manage Redundant or Trivial data for appropriate disposal.