Privacy Commissioner
Te Mana Matapono Matatapu

A Privacy Litmus Test

How comprehensive is your agency's risk management approach?

Context

What sort of information does your organisation collect about individuals?

- Is the information particularly sensitive?

As CE is my knowledge about privacy practice in line with modern practice and theory?

- Am I familiar with current thinking on personal information including Privacy by Design and the World Economic Forum on "Rethinking Personal Data" as the "new asset class"?

Governance and Leadership

Which governance group has a framework that reflects the importance of personal information to the organisation? Is there:

- A personal information management strategy
- A comprehensive privacy policy that reflects the operations of my organisation
- A risk management framework with appropriate weighting for privacy and the management of personal information

What level of accountability is there for privacy and data handling either as a primary responsibility or at least a major component of a senior executive level manager?

Which executive group has terms of reference that includes oversight of data management and privacy?

- Is that group knowledgeable about the personal data holdings of the business?

Privacy Programme

What type of privacy programme is provided for all staff?

- Is performance measured against the programme?
- Is privacy reflected in key competencies and performance indicators?
- Is privacy reflected in performance measures for senior staff?
- Is involvement in the programme mandatory for all staff?

How is privacy embedded in the key structural areas of the business?

- Are Privacy Impact Assessments used as a tool?
- Is privacy robustly considered before new products, services or processes are introduced?

Is there an adequately resourced privacy team to deal with complaints, access requests, corrections and compliance in general?

- What is the volume of work in this area?
- How effectively and efficiently is this work being done?
- How well is it integrated with any wider customer assistance and complaints programme?

Is there a plan and policy for data breaches/losses?

- Is the organisation ready for a large data breach?
- What measures are being taken to minimise or reduce the risk?

Culture

How is privacy seen by the executive team? Is it seen as a positive contributor to good business and efficiency?

What is the nature of the organisations privacy practice culture? How do we demonstrate that the privacy practice is respectable and appropriate?

Accountability

What do our customers/clients think of our data handling practices?

What measurement tools are used to track privacy performance against strategy, customer expectations and statutory responsibility?

Is a reporting and accountability framework in place that ensures leadership is well informed of the health of the privacy programme?