Privacy Fact Sheet

What are the good data privacy practices that can enhance a sustainable business?

All modern businesses need to know how to manage personal information well; whether the personal information relates to their customers or to their employees. It's not just a question of complying with the law under the Privacy Act 2020 (the **Privacy Act**). More fundamentally, how you handle information about people speaks to your businesses' values and purpose. Responsible and intentional data privacy practices are foundational elements of building trust and so we've set out some key elements of good data privacy practices below.

Transparency

Transparency is core to good data privacy practices. The principle is: "If you want me to trust you, you need to tell me what personal information you are collecting and how you will use it." The personal information that you handle might be limited to employee information collected as part of managing the employment relationship or captured on CCTV within your premises. It might extend to customer information collected as part of the e-commerce process, and used for marketing purposes. In all cases, it is fundamentally important to be transparent as to how you will use this personal information.

Privacy Notice / Statement

A key part of transparency is having a clear Privacy Notice / Statement which tells customers and employees what personal information is collected, how it is collected and how it will be used. This is a requirement under the Privacy Act. In order to ensure that your Privacy Notice / Statement is accurate and complete, you need to have a clear understanding as to how you are using personal information today (for instance, what marketing activities do you currently undertake?), and what you'd like to do in the future (for instance, would you like to be able to share personal information with third parties in the event you sell your business?). Ideally, the Privacy Notice / Statement should be forwards thinking, to support your ambitions for your business.

Privacy Policy

An internal privacy policy sets out further detail as to how your business will look after personal information, places limitations on its use and sets expectations for staff when they are handling personal information. It helps to guide decision-making on data privacy questions. It is also particularly helpful to have an internal-facing privacy policy in place in the event that something goes wrong (see below). If faced with a data breach or a complaint about your use of personal information, an internal privacy policy can demonstrate that your organisation takes data privacy seriously and that you have made best efforts to put good data privacy practices in place.

Responsible Individual

It's important to have a designated person who is responsible for privacy and data security and to manage compliance with your own privacy policy and with the Privacy Act. All organisations that handle personal information are required to appoint a Privacy Officer to deal with requests made for access to or correction of personal information, and to work with the Privacy Commissioner if a complaint is made about your business. For most businesses, the Privacy Officer role is not full-time and the responsibilities are typically given to someone who has an existing operational, legal, or compliance role.

Trusted third parties

Outsourcing

Many small to medium size businesses outsource elements of their operations (such as payroll, marketing, or customer database management) to third parties. Under the Privacy Act, any personal information transferred to a third party (for instance, in order to process payroll) is treated as being held by the organisation that collected the information. In this sense, the legal responsibility for that personal information remains with your business. This means that it is crucial to undertake robust due diligence to check that any third party vendors or suppliers are responsible in their data handling practices. It is important to have the right contractual arrangements in place to set clear expectations about how consumer data will be protected and to hold third parties to account.

Sending personal information overseas

Businesses are also responsible for ensuring that any personal information disclosed to organisations outside of New Zealand is adequately protected, and must be able to demonstrate that they have undertaken necessary due diligence before sending personal information overseas.

Acting responsibly when things go wrong

Data breaches

Data breaches are becoming increasingly common. Businesses of all types and sizes in New Zealand have been impacted by data breaches, including malicious cyber activity. A data breach can be very stressful for the affected business and can negatively impact customers and employees, as well as stakeholder confidence. These negative impacts can, in part, be mitigated by having a data breach response plan in place to help guide decision making, and next steps. At a minimum, the breach response plan should ensure that everyone in the business knows how to identify a data breach, and who to contact in order to manage it.

In some circumstances, for instance where the breach has resulted in the loss, theft or exposure of personal information, it may be necessary to communicate with the impacted individuals. The Privacy Act requires notification (to both the regulator and impacted individuals) where a breach may cause serious harm and provides a list of factors relevant to this assessment. Honesty is key; communicate early and ensure consumers understand what has gone wrong and what has been done to fix it. This can ultimately enhance trust.

Health check:

- Do you have an up-to-date Privacy Notice / Statement, accessible to both customers and employees?
- Do you have an internal policy setting out how you will ensure that personal information is used appropriately and stored securely, and have staff read it?
- Do you have someone in the organisation who can be responsible for privacy and security matters?
- Do you have a contract in place with any key third parties who handle personal information on your behalf? Did you conduct checks before giving them personal information?
- Does your team know how to recognise a data breach, and do you have a data breach response plan in place?

If you need any assistance with privacy or data protection matters, or would like access to PwC's Privacy Help Desk, please do not hesitate to contact:

Polly Ralph | Director
Head of Privacy & Data Protection Law
PwC Legal
E: polly.k.ralph@pwc.com
M: +64 27 374 2031

Rosa Henderson | Associate
PwC Legal
E: rosa.i.henderson@pwc.com
M: +64 27 248 3571