Ashurst

Customer Data: Are you managing the risks to reap the rewards?

25 July 2024

Customer data presents businesses with substantial opportunities, but also comes with notable risks. Understanding your data and the obligations surrounding this asset class is key to unlocking the value it can bring. In today's landscape, with competing schemes, and heightened scrutiny by governments and regulatory bodies, organisations face a raft of new and evolving legislation, regulation and guidance globally. There has never been a more critical time to understand your obligations, to ensure the secure and effective use of customer data.

Know your obligations

Customer data is a significant asset used by many organisations to undertake market analysis, drive pricing strategies, improve the customer experience, target marketing and gather competitive intelligence. The breadth and extensive scope of customer data maintained by organisations means there is a wide range of regulatory obligations that must be taken into account when collecting, using, storing or disposing of data. Legislative mandates, such as the following, necessitate careful management of individuals' information in different and competing ways:

1. Privacy Act
2. Workplace / Occupational Health and Safety legislation
3. Australian Consumer Law
4. Consumer Data Right
5. Corporations Act
6. Superannuation Industry (Supervision) Act
7. National Consumer Credit Protection Act
8. Income Tax Assessment Act
9. Anti-Money Laundering and Counter-Terrorism Financing Act
10. Regulatory guidance such as the Australian Prudential Regulation Authority's (APRA) CPG 234, 235, and CPS 230, and the Australian Securities and Investments Commission's (ASIC) RG 271.

Consider the retention of customer data – the current Privacy Act imposes a general obligation to destroy personal information an organisation no longer has a justifiable need to retain. However, other sources impose **minimum** retention periods for certain records. This intricate web of regulations highlights the challenges in compliantly collecting, using, storing, and disposing of customer data without a robust data governance and data risk management framework in place.

Regulators expect demonstrable oversight of customer data from organisations

Regulators are increasingly expecting entities to demonstrate how they handle personal information. For example:

1. ASIC has shown significant interest in regulating how data is collected and used for financial products, such as bank deposit accounts, superannuation and insurance.
2. Both ASIC and APRA hold accountable persons in banks, super funds and insurers responsible for data management, which encompasses data strategy, data architecture, data management frameworks and governance, data quality and issue management and data risk management, in addition to the status of data controls and data privacy, as a key function in the new Financial Accountability Regime (FAR).
3. The Office of the Australian Information Commissioner (OAIC) has repeatedly noted, both in guidance and determinations, that mapping and classifying data, and having visibility on data handling practices are important in meeting privacy obligations.
4. The Australian Competition and Consumer Commission's (ACCC's) Digital Platform Services Inquiry 2020-25 and the Privacy Act Review Report have both heavily focused on the complex data handling and sharing practices associated with digital marketplaces and digital advertising, including considering the maturity of understanding of organisations involved in these practices around their data handling.

Understanding your obligations, data and related governance frameworks and processes is critical to mitigating regulatory risk and scrutiny.

A generational change in privacy regulation is coming

In the wake of recent large scale data incidents, there is an increasing focus by the Australian public and regulators on how personal information and data related to individuals is collected, used, stored and protected. As a result of these concerns, the Commonwealth Government (and several States) are updating their legislation relating to the management of data, particularly the handling of personal information. The most salient example of this is the upcoming reforms to federal privacy legislation. These reforms will be a generational change in how personal information is collected, handled and secured, including how it is used to inform automated decision making processes that directly impact customers.

The questions you should be asking – and answering (with evidence)

- Are you able to demonstrate to regulators that you know what data you hold, where it is held, who can access it, the obligations attached to this data, and the legal basis to hold the data?
- Do your practices, procedures and systems allow you to meet your regulatory obligations with confidence, including those requiring recurrent data submission to regulators?
- Is your collection, use and retention of customer data in line with your organisation’s risk appetite and objectives?
- Significant privacy reforms are coming. Have you conducted a readiness assessment in your organisation to evaluate your current state of data risk management to proactively prepare for upcoming changes?

- Are you aware of where your organisation is using automated decision-making? If so, has this been integrated into your data governance and risk management processes (including risk assessments)?
- Informed data governance is essential to comply with your obligations. Do you understand the elements of a data governance policy and how to translate them in practice in a way that is tailored to your organisation's specific circumstances?
- A clearly defined and practised cybersecurity response to data breaches is key to managing cyber risk, an area of heightened regulator focus. Are your Board and executive team across cybersecurity risks and your key steps to adequately manage and respond to them?
- Who is accountable for data management, and are they aware of the reasonable steps they must take to fulfil their accountability obligations, including in the case of a data breach or suspected breach?

Want to know more to future proof your business?

Read our previous articles in this series:

- Are you future proof? How to keep on top of a rapidly changing risk and compliance landscape (5 April 2024)
- The perils and pitfalls of managing compliance obligations (9 May 2024)
- FAR from BEAR - Make sure you comply with the Financial Accountability Regime (FAR) (7 June 2024)

To learn about how Ashurst can support you to navigate the complex regulatory landscape, please contact us or visit our OMS webpage.

Authors: Morgan Spain, Partner; Chris Baker, Partner; Samantha Carroll, Partner; Sonia Haque-Vatcher, Partner; Leon Franklin, Director and Elizabeth Hristoforidis, Partner.