



Privacy and Personalisation:

A Balancing Act to Innovate the Customer Experience

APAC Report

Navigating the privacy-conscious era

The acceleration of digitalisation, coupled with recent changes in APAC's data privacy landscape, has made consumers more attuned to their data privacy rights. The EU's General Data Protection Regulation (GDPR) has transformed the way businesses in Europe operate. Looking at the EU's regulation, a number of APAC countries are drafting and updating their own regulations around data privacy. Approaches vary in terms of business-friendliness. In Australia for instance, the forthcoming framework aims to protect consumer privacy, while promoting market competition and commercial interests.

Executives must anticipate the impact of upcoming regulatory changes, future-proof their business operations and leverage this opportunity for improvement in honouring consumer privacy preferences as demand for personalisation rises. As data protection regulations continue to shift and brands brace for a cookieless future, businesses need to stay ahead of the curve to meet the ever-growing volume of online consumers. APAC shows exceptionally high consumer awareness of data privacy rights. In Australia, for example, **83%** of consumers have indicated concerns over cookies that track their online activity for targeted marketing.

Then we have personalisation. The growing demand for personalised engagement is more present than ever in APAC. Consumers in this region are considered some of the most **demanding** in terms of personalisation, expecting businesses to deliver seamless and tailored experiences throughout their entire digital journey, from interactions to communications and offers. They also display a high willingness to share their data in order to achieve this goal.

This level of openness should be encouraging for businesses. To give customers the experiences they want, which include personalised recommendations and exclusive offers, businesses must think in terms of mutual benefits. Personalisation and privacy do not have to be at odds. Approaching personalised service with a privacy-first mindset is key.

“ We understand that businesses are dealing with various challenges, including the decline in online performance and difficulties in attribution; businesses need to strike a balance between driving performance, while respecting people's privacy.”

Nadia Tan

Director of Business Ecosystem Partnerships for Asia-Pacific at Meta



Adapting to a cookieless future

The phasing out of third-party cookies comes at an opportune time. In Australia, it aligns with shifts in data privacy regulation, which means businesses can address multiple factors simultaneously when formulating a new data strategy. They are in a position to strengthen trust with customers by prioritising disclosure and consent. The key is to bring control and visibility back in-house – listening to customers' data privacy concerns and developing the strategies to meet them.

“Trust and transparency will be a top priority for businesses in a cookieless world,” says Marie-Louise Dalton, Vice-President of Marketing, Asia-Pacific & Japan at Tealium. “As brands rely more heavily on first-party data in their marketing strategies, establishing a trusted value exchange with consumers will be more important than ever.”

While marketers have long relied on third-party tracking cookies to target ads, shifting to a first-party data strategy will allow businesses to drive specific targeting and more genuine and useful content, while respecting consumer privacy. Unlike third-party data, first-party data is collected and controlled solely by the brands, giving businesses the opportunity to align privacy requirements with marketing needs.

Meta's application programming interface (API) tool, the Conversions API, is a tool that enables businesses to easily share on-site first-party data gathered from consumers. **“This effectively allows you to preserve data-driven marketing and optimise performance, while respecting people's privacy,” Nadia added.**

However, taking the first step towards a data-first strategy may come as a challenge to many. With an influx of customer data from multiple sources, generating high-quality insights can be slow. Often, data from disparate systems results in a lack of visibility into what kind of data it is, where the data is coming from, and where it's being used. When vast amounts of customer data are collected across various touchpoints and managed within silos, businesses are not able to realise its full potential. It is not possible to achieve data protection that promotes hyper-personalisation in a vacuum.

This is where a customer data platform (CDP) like Tealium, a Meta Business Partner, comes into the picture. A CDP can help businesses streamline all the data captured from multiple sources into one place, stitching together a holistic single view of each customer and providing scalable benefit in conjunction with a solution such as Meta's the Conversions API.

Australian internet service provider, Dodo, worked with Tealium to use Meta's the Conversions API to improve its campaign measurement and performance. The tool helped Dodo earn 26% more in incremental sales and achieve a 23% higher conversion rate.

Companies investing in their first-party data strategy through CDP and data management tools are those leading their industries into a new era of privacy and personalisation. For Tealium, privacy and consent sit at the core when collecting first-party data. Maintaining the security of data is key to building and retaining customer trust throughout the entire customer lifecycle.

Similarly, Nadia shares that through such tools, Meta aims to provide businesses performance solutions that respect privacy choices. The company believes that such experiences will provide customers, businesses and creators with new opportunities and ways to connect and grow.

“As brands rely more heavily on first-party data in their marketing strategies, establishing a trusted value exchange with consumers will be more important than ever.”

Marie-Louise Dalton

Vice-President of Marketing, Asia-Pacific & Japan at Tealium



Shifting to a first-party data strategy

Even with a CDP in place, brands must earn their customers' trust and permission to collect robust, first-party data. Transparency and honouring customer preferences are key. Marketers need to talk to customers transparently about how their data will be handled, while utilising data in line with customer preferences to provide meaningful experiences. These could include special offers, such as loyalty programs, exclusive discounts and personalised experiences. When Accenture Interactive surveyed 8,000+ consumers globally in 2021, 73% of respondents said they would be willing to share more personal information if brands are transparent about how it is used, up from 66% in 2018. Such value exchanges encourage transparency and trust between the brand and the consumer.

“We have an open relationship with customers on our privacy and data usage policy. I think it's more important to talk to and involve customers when optimising the onboarding and consent flow rather than working on technical workarounds or band-aid solutions. We've seen opt-in rates well above average as a result,” says David O'Rorke, Head of Performance Marketing at The Iconic when it comes to implementing data strategies.

73%

of respondents said they would be willing to share more personal information if brands are transparent about how it is used.

The shift to a first-party data strategy also calls for a holistic measurement system in the new age of marketing. Achieving both accurate and practical measurement will require bringing together multiple measurement solutions, including attribution, sales & conversion lift and marketing mix modelling (MMM). Tim Higgins, Customer Insights & Growth Lead at Accenture, proposes a shift in thinking: to use measurement not to judge success, but to inform better holistic decision making. The new normal of the privacy age emphasises growth and customer advocacy through measurement and flexibility. A robust measurement framework is also critical in influencing cross-functional teams towards a unified vision.

Balancing privacy obligations with enhanced personalisation revolves around three key principles: transparency, choice and consent, and data minimisation and anonymisation. To gain robust first-party data, brands will need to talk to their customers transparently about how their data will be handled and provide them with real benefits in exchange for sharing it. The ultimate goal is to innovate to drive personalisation and performance, while at the same time respecting people's choices about how their data is being used to drive the ads they see. In other words, asking for permission to share data across sites to enable ads-based free services.



Powering performance by putting privacy first

Achieving such balance starts with having the right privacy-enhancing technologies in place, including secure multi-party computation, on-device learning and de-identified data. On the security front, secure multi-party computation enables businesses to learn together by only sharing encrypted or unintelligible data, while de-identified data adds a further layer of privacy protection by reducing the risk that any individual can be identified. Personalisation can be enhanced through on-device learning, which finds useful patterns in historical data in order to make predictions; identifying ads that would be most relevant to a person, while ensuring the individual's data remains on their devices.

With the right technology stack at the heart of a first-party data strategy, businesses will have the ability to take data from various new sources, feed that data into advanced technology, such as machine learning, and ultimately scale for future growth. Although switching to a first-party data strategy won't happen overnight, investing in a CDP will pave the road towards enabling both personalisation

efforts and meeting the growing demands of privacy regulations and customer needs. By striking the right balance between privacy and personalisation, brands will slowly gain their customers' trust and build stronger brand loyalty.

Transparency is paramount. Whether you're in retail, travel, financial services or healthcare, consumers expect the same thing: seamless customer experiences tailored to their preferences that can offer both value and relevance, as well as the ability to trust that their personal data is in good hands. Help consumers understand how your business uses their data and how you keep it safe. Stay informed about data privacy regulations and evaluate how they may impact your business to take proper, timely action. Most importantly, let your customers choose. Put the ball in the customer's court. Invite and enable them to make choices that define how personalised their experiences will be across your digital platforms.

Integrating consent management into personalisation strategies

The APAC privacy landscape is changing and customer needs continue to evolve, as individuals are more aware of their data privacy rights than ever before. For businesses, privacy should not be seen as a barrier. Instead, to future-proof a business, consent and transparency need to be built into any personalisation strategy from the start. They are the building blocks to gain and retain trust in a world where data is increasingly commodified.

When addressed properly through transparency and consent, first-party data collected by a CDP, through a tool like Meta's the Conversions API, can gather relevant data, standardise it and syndicate data collection to drive better customer insights. Personalisation is then expected and appreciated as customers will see the value in their data exchange.

Here are practical steps to follow in establishing a privacy-compliant data collection and management strategy:

- 1** Prepare for the shift to first-party data by changing your mindset, or begin investing in fit-for-purpose data management tools.
- 2** Determine what kind of first-party data you need to deliver a valuable, hyper-personalised experience for your customers and focus on acquiring that.
- 3** Develop a first-party data strategy where you understand and honour customer privacy preferences.
- 4** Integrate tools that add transparency, control and efficiency in the management of personal customer data to protect consumer privacy.
- 5** Connect with a CDP like Tealium for a privacy-enhancing technology solution that drives personalisation and performance.





Tealium connects customer data across web, mobile, offline and IoT, so businesses can better connect with their customers. Tealium's turnkey integration ecosystem supports more than 1,300 built-in connections, empowering brands to create a complete, real-time customer data infrastructure. Tealium's solutions include a customer data platform with machine learning, tag management, an API hub and data management solutions that make customer data more valuable, actionable, privacy-compliant and secure. More than 850 leading businesses throughout the world trust Tealium to power their customer data strategies.

For more information, visit

www.tealium.com

