Consumer privacy: A business imperative in the digital age

In today's data-driven world, one of the biggest challenges that businesses face is managing data. With increasing volumes of data being collected and processed, ensuring consumer data privacy becomes a constant challenge. Data breaches are not only harmful to businesses and organizations but also affect consumers, who often suffer financial and emotional damages, ultimately leading to a loss of consumer confidence and trust. In response to recent prominent data breaches and growing awareness about personal privacy, regulators have enacted laws and regulations to protect and uphold the rights and privacy of individuals. This article outlines the importance of data privacy, the challenges associated with data compliance, and the necessity of cultivating a culture of privacy awareness.

Consumer data: A powerful tool in the hands of consumer businesses

Consumer data is the information trail left by consumers when navigating the digital world or trading online; this includes personal preferences, demographic data, behavioral patterns, location-tracking, and other forms of personally identifiable information. Consumer data can provide businesses with invaluable insights to better understand consumer preferences, trends, and behaviors. It can help enhance the user experience, develop new products and services, and personalize advertising.

However, as businesses collect, store, process, share, and even sell more and more consumer data, they also face a significant duty—the duty to safeguard the privacy of consumers who become increasingly aware of their personal privacy. Data protection and privacy can be a source of differentiation and customer satisfaction, contributing to business retention and sustainability.

The General Data Protection Regulation (GDPR): Five years later

It has now been five years since the GDPR in the European Union (EU) came into effect as one of the strongest and most comprehensive data protection regulations.[1] The GDPR provides greater protection and rights to individuals while placing limits on what organizations can do with personal data. Personal data is at the heart of the GDPR, which has transformed the way businesses can handle consumers' personal information. There are strict regulations on how businesses can collect and process personal data, and heavy fines can be imposed in case of non-compliance.[2] The GDPR has not only changed the European data privacy scene but has also influenced the world, as it also applies to businesses that are based outside of the EU.[3]

Data privacy: The key to building consumer trust

In a digital world, data privacy stands as one of the key pillars for maintaining consumer trust and fostering increased loyalty. As consumers become more aware and sensitive about their data privacy, implementing robust measures can give businesses an edge over their competitors and help forge strong consumer relationships.

Transparent data practices, explicit consent mechanisms, and stringent security measures form the foundation for establishing trust with consumers.

Organizations that explain their data practices to consumers in easy-to-understand language clearly demonstrate their commitment to transparency, fostering trust. Seeking explicit consent from consumers grants them freedom from intrusion into their private data, boosting their confidence. Building robust data security measures further reinforces consumer faith by assuring their personal information and financial data are protected from potential threats and breaches.

Data privacy compliance: The challenges

Organizations face numerous data privacy challenges, starting with the cost of privacy as a function; becoming privacy-compliant requires a considerable investment in time, resources, and effort. Additionally, there is the cost of maintaining data privacy, as companies may invest in key security technologies. Data classification is another challenge, as organizations must identify and classify personal data within their systems, a process that can be both time-consuming and costly, particularly for consumer businesses with large amounts of data.

Cross-border data transfers present an additional challenge, particularly for global businesses. With diverse data protection regulations in various countries, organizations operating internationally must comprehend and adhere to the data compliance requirements specific to each jurisdiction.

However, the biggest challenge in data privacy remains human error. The World Economic Forum's Global Risks Report 2022 highlighted the critical challenges related to cybersecurity and data breaches, with one alarming statistic: 95% of data breaches were caused by human error.[4] Addressing this issue requires significant investment in training and education, robust policies and procedures, and technology solutions such as data loss prevention.

Data ethics: Embracing ethical data practices

Ensuring the ethical collection, storage, and analysis of consumer data is not only a legal requirement but also a moral obligation. Ethical data measures are critical to prevent bias in data collection and analysis, as well as discrimination and other harmful consequences. Prioritizing ethical data practices allows businesses to cultivate trust, mitigate risks, and bolster their reputation, thereby contributing to their long-term success and sustainability within an ever more data-centric world.

As businesses incorporate technology and data at the core of their business strategy, consumers will remain loyal to the brands they trust. Data ethics is a fundamental part of this process.

Building a culture of data privacy: The importance of education and collaboration

While approaching data privacy compliance as an independent function can significantly help achieve privacy goals, from operational efficiency to legal compliance and consumer trust, all internal stakeholders, including legal teams, IT teams, HR teams, and marketing and sales teams, must work hand in hand as the primary generators and users of consumer data.

Furthermore, every other employee must be trained and equipped with the knowledge of ethical data practices. Building trust requires a joint effort to ensure the responsible use and protection of data. A fundamental component of this effort involves educating users about the best privacy practices by raising awareness about their rights, the types of data collected, how it is utilized, and the measures in place to protect it.

Case studies: The cost of data breaches

Google's privacy controversies

The first significant fine under the GDPR was levied against Google with a EUR50 million (US$52.9 million) fine from the French data protection regulator, the Commission Nationale Informatique & Libertés (CNIL). The fine was issued for two main reasons: Google's failure to provide sufficient information to users regarding how it utilizes data collected from 20 different services, and not obtaining proper consent for processing user data.[5]

Meta's violation of GDPR rules

Meta, the owner of Facebook, was fined by the Irish Data Protection Commission (DPC) for violating the GDPR by transferring personal data of EU users to the US without adequate safeguards.
The fine of EUR1.2 billion was the largest GDPR fine ever and was imposed following a binding decision by the European Data Protection Board (EDPB), which resolved a dispute between the DPC and other EU data protection authorities.
Meta was also ordered to stop transferring user data to the US by October 2023 and to delete any data that was transferred unlawfully since July 2020.[6]

Facebook's data scandal

The Facebook/Cambridge Analytica scandal was a major data privacy breach that took place in 2018. It involved the misuse of personal data from millions of Facebook users by a political consulting firm called Cambridge Analytica. This firm used the data to influence elections and campaigns worldwide, without the users' consent or knowledge. The scandal sparked public outrage, triggered regulatory investigations, and significantly tarnished Facebook's reputation and trust.

In December 2022, Facebook's parent company, Meta (formerly known as Facebook), agreed to pay US$725 million to settle a class-action lawsuit related to the scandal. This settlement represents the largest in a US data privacy class action and encompasses all US Facebook users who had active accounts between May 2007 and December 2022.[7]

Yahoo's data breach

In 2016, Yahoo, one of the largest internet companies in the world, disclosed two massive data breaches that occurred in 2013 and 2014. The breaches affected over three billion user accounts, exposing names, email addresses, passwords, and security questions. The breaches were attributed to state-sponsored hackers and resulted in a US$350 million cut in Yahoo's sale price to Verizon.[8]

These case studies provide valuable insights into the real-world effects of data breaches in consumer businesses. The impact of data breaches can be substantial, and beyond the financial fines and legal repercussions, the reputation damage can erode customer trust and loyalty, leading to further loss of profits and market share. Prioritizing data protection ensures legal compliance, financial stability, and sustained reputation, while strengthening trust between businesses and consumers.

By **Ikram Moulila**, Director, Financial Advisory, Deloitte Middle East

Endnotes

1. Source: General Data Protection Regulation (GDPR) – Official Legal Text – Key Issues. Link: https://gdpr-info.eu/issues/.
2. Source: General Data Protection Regulation (GDPR) – Official Legal Text – Fines / Penalties. Link: https://gdpr-info.eu/issues/fines-penalties/.
3. Source: General Data Protection Regulation (GDPR) – Official Legal Text – Third Countries. Link: https://gdpr-info.eu/issues/third-countries/.
4. Source: World Economic Forum – Global Risks Report 2022 – Page 52. Link: https://www.weforum.org/publications/global-risks-report-2022/
5. Source: European Data Protection Board, 21 January 2019 - The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | European Data Protection Board (europa.eu).
6. Source: European Data Protection Board, 22 May 2023 - https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland.
7. Source: Court filing of the proposed settlement agreement between Meta and the plaintiffs, which was disclosed on 23 December 2022 - https://www.justice.gov/crt/case-document/file/1514126/download.
8. Source: Reuters, 4 October 2017, based on Yahoo official announcement - https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1.

In a digital world, data privacy stands as one of the key pillars for maintaining consumer trust and fostering increased loyalty