Businesses and consumers must protect personal data in the digital era

Forget gold or oil, personal data has become our most valuable commodity in what is an ever-evolving digital society. An increasingly valuable commodity, data is now used to purchase items or conduct business, and personal data such as names, email addresses, telephone numbers, bank account and identification numbers are estimated to be worth a total industry value of around $224bn.

Image supplied

Unfortunately, incidents like the Cambridge Analytica fiasco just a few years ago, which saw the political consulting firm harvest (likely) more than 87 million Facebook users' data without their knowledge or permission, quickly unmasked the dark side of personal data collection and its misuse.

"The dangers of the exploitation of the massive amounts of personal data that are collected, stored, and shared by businesses, government agencies, financial institutions and even social media platforms by malicious actors spurred on nations across the globe to adopt more stringent data governance regulations and privacy policies," says Keletso Mpisane, head of MiWay Blink.

The European Union was the first to introduce modernised data privacy law through the adoption of the General Data Protection Regulation (GDPR) in 2016. In Africa, 19 countries have introduced data protection and privacy laws, with the laws of six of these countries still in draft form.

And, in South Africa, the country enacted the Protection of Personal Information Act (PoPIA) to regulate the collection, use and processing of personal data in 2020.

Personal data helps businesses to provide customers with greater value by providing improved customer service and experiences. With organisations increasingly digitalising their businesses to cater to the personalised needs and expectations of consumers through digital applications and touchpoints, the question for consumers is - how protected is their personal information really?

Putting the consumer in control: the power of consent

15 Nov 2023

While data privacy laws such as PoPIA endow organisations with the responsibility to ensure that personal information is stored safely and is not accessible to individuals who would use it with malicious intent, it does not provide consumers with any guarantees that their personal data will always be secure.

Cyber criminals are becoming increasingly sophisticated with greater access to tools and resources that help them to breach what is thought to be secure systems and networks. As such, the number of both attempted and successful breaches are increasing. In fact, South Africa's Information Regulator received more than 500 notifications of data breaches or security compromises since October 2022 to date.

Additionally, IBM's latest annual Cost of a Data Breach report found that the average cost of a data breach for South African organisations reached a record high of R49.45 million in 2023, an 8% increase in the last three years, and a 73% increase since the country was added to the report just eight years ago.

"We can see that it is in most organisations' best interests to employ robust security protocols that protect sensitive customer data against cyberattacks, malware, ransomware, hacking and a number of other cybercrimes as not only can such incidences lead to many difficulties like loss of business-critical data and costly downtime, it also means loss of trust from customers and consumers," adds Mpisane.

"Nonetheless it's also important that consumers are careful and cognisant of what information they are sharing and with who. If our personal data is a valuable commodity, then we must be sure that we are not just giving it away unknowingly and for free."