



The Rise of Data Privacy in the Age of Technology

After the spate of large data scandals and breaches widely publicised in 2018, data protection has become a common topic of discussion amongst businesses and their consumers. With the most recent implementation of the GDPR (The General Data Protection Regulation), data, its value and the protecting of it has become an integral part of any business strategy discussion. Consumers' trust in the previous data-driven business model plummeted and as a result, businesses have realised that to retain customers they need to make fundamental changes to the way that personal data is collected, managed and shared.

With the increasing need to conform to evolving worldwide privacy norms, and the economic imperative to encourage domestic innovation, businesses must find new and more secure ways to balance the way in which they acquire and access customers.

To do this one must look at and follow a basic design of a modern, balanced and flexible privacy framework. Typically, this framework is governed by 4 parts: an overarching law; a core set of data protection, security principles as well as an unbiased and independent authority with effective powers to supervise and enforce the rules. This framework will restore a baseline level of trust for consumers and reassure them that their data is being used properly. This ensures that by protecting customers privacy fosters maximum business success as customers feel less at risk.

Reaping the Reward

It is interesting to note that associations who put resources into developing their information protection practises are currently gaining substantial business profits

Cisco conducted a Data Privacy Benchmark Study in 2019 and according to the study, there is a direct link between good privacy practice and business benefits. Respondents reported shorter sales delays as well as fewer and less costly data breaches.

Also noted by the study were that 59% of organisations reported meeting all or most requirements, 29% expect to do so within a year, and 9% will take a little longer a year.

"Data is the new currency, and as the market shifts, we see organisations realising real business benefits from their investments in protecting their data," said Michelle Denedy, Chief Privacy Officer, Cisco.

A Global Phenomenon

Data and the protection of it not only affected those in the EU. Worldwide, organisations and consumers recognised the need for change. More than 3 200 worldwide security and protection experts in 18 nations and from various significant industries reacted to the Cisco study about their organisations protection practices.

It was discovered that:

87% of companies are experiencing delays in their sales cycle due to customers' or prospects' privacy concerns, up from 66% of the previous year.

Businesses realised that implementing stricter data protection measures across their organisation had far reaching effects. Interesting, only 37% of GDPR-ready companies experienced a data breach costing more than \$500 000, compared with 64% of the least GDPR-ready companies.

As quoted by Peter Lefkowitz, Chief Digital Risk Officer, Citrix Systems and 2018 Board Chairman, International Association of Privacy Professionals (IAPP):

"This research provides evidence for something privacy professionals have long understood, that organisations are benefiting from their privacy investments beyond compliance. The Cisco study demonstrates that strong privacy compliance shortens the sales cycle and increases customer trust."

Embrace the Change

The rising importance of privacy regulations constituted a worldwide shift in consumer awareness. As increased concerns amount around data privacy issues, the casual way in which data is systemically captured and handled has significantly changed. As we progress into the new and improved digital era, we are bound to face more need to regulate our existing data collection policies and implement stricter measures. But as businesses and consumers we ultimately face the same unique goal, we want to feel empowered to take ownership of our data and protect it like the valued commodity it is. To do this, businesses must embrace the post-GDPR landscape by reprioritising their existing IT landscape, adjust their security strategies and standardise on advanced security solutions. By doing this, businesses will ultimately reposition themselves, to their consumers, as trustworthy organisations who value data protection as much as they do.

References

<https://www.itweb.co.za/content/GxwQD71A99O7IPVo>