WERKSMANS
ATTORNEYS

REGULATORY | TECHNOLOGY & INNOVATION

Road block ahead! Are data protection laws stifling technological innovation?

4 August 2022 *7 min read*

by Ahmore Burger-Smidt, Head of Data Privacy and Cybercrime Practice, and Siyabonga Galela, Candidate Attorney

Oh, where the time has gone! It has been four years since the European Union's flagship data privacy legislation, the General Data Protection Regulation (**GDPR**), came into force.[1] Similarly, 1 July 2022 marked the first anniversary of the implementation of South Africa's Protection of Personal Information Act 4 of 2013 (**POPIA**); and South Africa's crossing of the proverbial 'data privacy Rubicon' in respect of the compliance deadline imposed by the legislation.[2]

Both pieces of legislation are ground breaking to the extent that they represent governments' recognition of the need to establish comprehensive data protection regimes that facilitate the protection of the fundamental right to privacy at both the national and international levels.

The fourth industrial revolution (also known as 'Industry 4.0') is characterised as an exponential pace of technological change that has, and will continue, to facilitate a rapid and fundamental disruption that impacts the way we work and live. Unsurprisingly, it is against this backdrop of fast-paced technological development that questions around the longevity of data protection legislation such as the GDPR and POPIA are starting to arise.[3]

A principled approach to data protection

The GDPR, as well as national data protection legislation such as POPIA, was instituted in order to accommodate developments in new technologies such as artificial intelligence (**AI**), machine learning and cloud computing.[4] However, in implementing such legislation, it appears that Data Protection Authorities around the world have taken the position that once principles of lawfulness, fairness and transparency are incorporated into data protection legislation, such legislation will be "future-proof" insofar as it addresses concerns relating to the protection of user privacy.

The data-privacy compliance journey is not an idle one. For example, POPIA triggers various on-going obligations that necessitate a constant review of the application of POPIA. Instead of setting hard-'n-fast rules regarding the manner in which an individual's right to privacy is protected, the legislator has chosen to focus more on establishing general principles that underpin data protection.

This approach is understandable given the multitude of contexts within which an individual's personal information may be processed in Industry 4.0. Accordingly, there is very little of what technology could make possible, that data protection legislation would outright prohibit.[5]

Be that as it may, there appears to be a lack clarity as to how such data protection principles may be applied when considered in the context of the enforcement of data protection legislation.

A study conducted by the National Bureau of Economic Research reported that just over 32% of apps available on the Google Play Store were induced to exit the market; while the entry of new apps in the market fell by half between the period of 2016 to 2019, as a result of compliance concerns with data privacy legislation and the risk of large fines.[6]

Domestic data protection regimes

Part of the problem might be that both developers and users are uncertain as to what practices would be tolerated under their domestic data protection regimes and where applicable, cross-border interactions between such regimes.[7] For example, in Europe, several businesses have faced penalties for violating citizens' data rights when using new technology.

In 2019, the Dutch Data Protection Authority imposed a fine of €725 000 on a company that processed biometric fingerprint data when less intrusive means of processing were available.[8] In Hungary, the Budapest Bank was fined approximately €650 000 for using voice-analysis AI systems to assess the emotional state of customers who telephone the bank's call centre, and monitor its handling of customer complaints.[9]

More recently, the U.K. Information Commissioner's Office fined Clearview AI more than £7.5 million for collecting people's images from internet and social media sites without their knowledge or consent in order to create a global online database that could be used for facial recognition in criminal investigations.

The South African approach to conducting data-related investigations and the imposition of fines is even more uncertain given the infancy of the Office of the Information Regulator (**Regulator**); and is yet to show its teeth in respect of its handling of data breaches (and complaints related thereto) and willingness to set precedents relating to what the enforcement of POPIA will look like from a practical perspective.

Data protection and privacy regulation: A roundup of developments in Africa in 2021.

Conclusion

From a business development perspective, companies need to develop a deeper understanding of how to mitigate risks and/or violations related to the protection of personal information. In other words, processors of personal information need to improve their awareness of regulatory and legislative enforcement trends in order to understand the impact of their own organisations (and whatever technological developments that may arise therefrom).[10]

One way to achieve this is to carry out data impact assessments that evaluate the new technology in the context of compliance with POPIA. Afterall, being able to justify business decisions from a data privacy perspective, as opposed to implementing new technologies without considering data protection legislation, is integral to not only ensuring compliance, but also defending claims.

Be that as it may, companies and organisations cannot improve their awareness of the "*why and how*" of data protection without input and guidance from the Regulator.

To this end, the Regulator needs to adopt a proactive approach to helping companies and individuals understand POPIA beyond the implementation of generic privacy policies. This can be done via the implementation of new regulations and/or publishing of directives that provide further guidance as to, *inter alia*, what is expected of data processors and operators during the course of their collection and processing of personal information.

When data protection rules are difficult to understand and/or apply in practice, organisations tend to either fall into the trap of believing that avoiding such riles is more pragmatic;[11] or adopt the view that the mere adoption of a privacy policy is sufficient to guard against the infringement of data privacy rights. In the words of one Richard-Coggan, "*...it is often very difficult to achieve meaningful compliance when you are trying to bolt it on as afterthought.*"[12]

'Think privacy' ought to become the mantra informing all business procedures and processes today, tomorrow and every day thereafter.

Footnotes

[1] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[2] 1 July 2021.

[3] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[4] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[5] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[6] R Janben et al. "GDPR and the lost generation of innovative apps", accessed on 26 May 2022.

[7] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[8] Autoriteit Persoonsgegevens "Fine for company for processing fingerprints of employees", accessed on 27 May 2022.

[9] European Data Protection Board "Data protection issues arising in connection with the use of Artificial Intelligence", accessed on 26 May 2022.

[10] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[11] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

[12] N Hodge, "Four years of GDPR: New tech testing data privacy law's longevity?" Compliance Week, accessed on 25 May 2022.

Ahmore Burger-Smidt

Head of Regulatory

View Profile