WERKSMANS ATTORNEYS

REGULATORY

Sticks, straws and bricks: POPIA compliance strategy & governance framework

4 August 2022 *5 min read*

The Protection of Personal Information Act, 4 of 2013 (POPIA) is now over a year in full effect. Indeed, the POPIA compliance process has not come easy for many organisations. This is partly because of the nuanced nature of many businesses which can create a difficulty in properly interpreting the legislation.

Although South Africa lacks the jurisprudence due to the infancy of POPIA, we are still able to look abroad to jurisdictions with similar data protection laws for guidance.

Information Regulator's enforcement initiatives in South Africa

An important recent development that ought to be expected to impact on the Information Regulator's enforcement initiatives in South Africa is that of regulator's entering into memoranda of understanding (MOUs) to join forces in the investigation of data privacy transgressions. This was the case in the recent matter involving Clearview AI.

Clearview AI is an American company which provides a service that allows customers, including law enforcement, to upload an image of a person to the company's app which is then checked for a match against all the images in the database. Clearview AI's database is comprised of multiple images of people from all over the world, collected from a variety of websites and social medial platforms.

In July 2020, the Information Commissioner's Office (ICO) of the United Kingdom (UK) commended a joint investigation with the Office of the Australian Information Commissioner (OAIC) into Clearview AI's alleged privacy transgressions.

[1] The OAIC focused on the Australian Privacy Act and found that Clearview AI had failed to take reasonable steps to implement measures to ensure compliance with the Australian law when conducting its activities. Further, Clearview AI was found by the OAIC to have transgressed the rights of data subjects by unlawfully processing their biometric information. This resulted in a number of declarations by the OAIC, including the prohibition on Clearview AI to continue the impugned activities.

The ICO fined Clearview AI £7,552,800 for the following privacy transgressions:

- failing to use the information of UK residents fairly and transparently;
- failing to have lawful reasons for processing the information;
- failing to have an adequate data retention process (i.e. information was being kept indefinitely with no legal basis);
- failing to meet the higher data protection standards required for biometric information; and
- failing to have an adequate or enabling objection process for data subjects.

In another instance, Clearview AI was fined €20million by the Hellenic Data Protection Authority (HDPA) of Greece.[2] In particular, the HDPA fined Clearview AI for the following violations:

- failing to appoint a representative in the EU;
- failing to have a lawful basis for the processing;
- failing to be transparent in its processing activities; and
- failing to give effect to right of access of data subjects.

It is important to note the significant role of joint investigations and MOUs between data protection regulators in enforcement against global organisations. In the Clearview AI matter before the ICO, the following instruments informed the joint investigation:

- Australian Privacy Act and the UK Data Protection Act 2018;
- the data protection MOU between the ICO and the OAIC; and
- the Global Privacy Assembly's Global Cross Border Enforcement Cooperation Agreement.[3]

This demonstrates the heightened risk for organisations when regulators start working together. Accordingly, an organisation's privacy strategy and framework cannot be built with sticks and straws. It will be the house made of bricks which will not be blown away by the Big Bad Wolf. Accordingly, you should have a strong and robust privacy regime that is capable of withstanding scrutiny from the Information Regulator.

Read more about: Data breaches in South Africa post POPI...Any lessons to be learned?

Interpretation remains one of the key questions regarding POPIA implementation and compliance. However, with international jurisprudence we can look abroad to anticipate how certain issues may be approached in South Africa. All organisations should be prudent when it comes to POPIA compliance.

In particular, global organisations, especially those which do not have a physical presence in South Africa, should note that the lack of a physical presence may not be enough to escape POPIA scrutiny. This is because POPIA's application extends to organisations outside of South Africa which, in any event, use or process personal information in South Africa by various means (e.g. digitally or physically). Consequently, they too should comply with POPIA.

South Africa may start to see the Information Regulator entering into MOUs with other regulators similar to the arrangement between the ICO and OAIC. Furthermore, it is expected that the Information Regulator will join the Global Privacy Assembly's Global Cross Border Enforcement Cooperation Agreement.

Such a development would undoubtedly bolster the Information Regulator's investigative ability and enforcement effectiveness which would necessitate an equally robust approach to compliance by organisations.

Footnotes

[1] Hellenic DPA fines Clearview AI 20 million euros

[2] OAIC and UK's ICO open joint investigation into Clearview AI Inc.

[3] This helps to facilitate cross border information sharing and enforcement cooperation between data protection and privacy authorities.

Ahmore Burger-Smidt

Head of Regulatory

View Profile