POPIA in the age of AI

The artificial intelligence (AI) market is predicted to reach revenues of $156 billion by the end of 2020, according to IDC, with the largest segments being application and enterprise relationship management (ERM) at 20% and 17% respectively.

Matthew Mckie, co-founder and chief analytics officer at Omnisient

The scale of AI growth alongside developments in automation, machine learning, deep learning, and the Internet of Things is equally driving the creation of extraordinary volumes of data. In fact, research has found that the number of digital bits produced every year could exceed the number of atoms on the planet by the year 2245. But as data grows and AI interprets and organisations analyse, so does the risk – the risk of non-compliance with regulations such as General Data Protection Regulation (GDPR) in Europe and the Protection of Personal Information Act (POPIA) in South Africa.

As of 2021, companies in South Africa will have to embed POPIA compliance into their systems and processes and they have to manage personal data in AI applications incredibly carefully. In fact, according to Matthew Mckie, co-founder and chief analytics officer at Omnisient, organisations can't assume that AI systems are compliant as they risk sleepwalking into breaking regulations.

"AI systems can often be very complex, but the regulations are clear – no organisation can use personal information without consent. They can't create models or link data or develop solutions that leverage personal information to connect the dots or unpack insights," he adds. "From the outset, organisations have to ensure that they are compliant and that their investment into analytics and intelligence is designed to fit the lay of the legal land."

The risk lies in analytics. The use of data to drive business processes. AI can potentially become a black hole down which falls unsupervised data analysis and that runs the risk of using the data to do things for which it was not intended. That's the nature of AI and data regulations have been designed specifically to minimise this risk and protect personal information.

"Data privacy regulations such as POPIA regulate the use of personal information that's linked to an identifiable person, information that was originally collected with a specific purpose in mind," explains Mckie. "Technology then takes the data and whisks it off for use in different areas of the business and often isn't de-identifying the data in the process. The result is information that's of value to the business but not always compliant with regulation."

Unfortunately, many organisations don't realise that they are putting themselves at risk of breaking with regulation. Analytics are complex, data is swirling in lakes and many companies are unaware of where their data is located, what data their models are based on, and how information is being used. This is particularly challenging in sectors where they are customer-facing – AI takes the data to create experiences that can transform how organisations engage with their customers, but this may cause problems further down the line when customers object to this level of scrutiny.

And, of course, there is the perennial risk of a breach, where data is stolen and personal information compromised and the organisation left holding the fine and the tatters of its reputation.

But what business is going to turn away from the value of data to avoid the risks? None.

"The solution isn't to ditch the data and lose the insights but to rather focus on a solution that's capable of removing the person from the information," concludes Mckie. "Instead of compliance risk and regulatory fines, use software that de-identifies the data and removes the need for consent of use. If there's no personal information, then there is no risk. It's a simple solution to a complex problem because not needing consent until the data is actioned saves time, money, and avoids regulatory issues.

Simple indeed. De-identified data can be used as effectively to achieve the same results but there's no privacy risk and the organisation is immediately compliant with ongoing regulation. AI is of immeasurable value to the organisation, particularly in the current climate, so don't throw the proverbial baby out with the bathwater in search of compliance, just de-identify the data.