KPMG

Ethical use of data

The fair processing of personal information requires organisations to put themselves in the hearts and minds of data subjects…

It is no big revelation that knowledge **about** us can be used to exert power over us. But today, this point is even more true, and more relevant. With the evolution of data science and algorithmic prediction, we are prodded and influenced in countless ways.

Entrusting organisations with so much information about themselves also makes customers vulnerable. If organisations are careless with such information, customers are at risk of identity theft and cyber fraud. If organisations are aggressive with such information, customers suffer intrusions into their privacy. The rights of customers may even be violated when algorithms fed with their information inappropriately discriminate against them.

The financial services industry collects a sizable amount of information about us. Banks know where and when their customers buy their groceries, how much their homes cost, whom and how much they owe, and where they holiday. Insurers know their customers' medical conditions, where and when they exercise, the contents of their homes, and these days even how fast they drive.

Of course, this information can be used to better serve clients. It allows service providers to offer goods and services which are relevant to customers. It may also be used to improve the overall customer experience (e.g. imagine how much more efficient an insurance application process could be if the insurer could gather data using big data analytics).

A recent survey conducted by KPMG US , found that 68% of respondents are concerned about the level of data being collected by business and 40% of respondents don't trust companies to use their data ethically. One of the key challenges for organisations today is to ensure that they collect and use data both lawfully and ethically. But what does that entail?

The fair processing of personal information requires organisations to put themselves in the hearts and minds of data subjects…

While the Protection of Personal Information Act No. 4 of 2013 ("POPIA") underpins many of the principles synonymous with ethical processing, organisations should consider international guidance and leading codes of conduct in checking its moral compass. Organisation should ask themselves "would data subjects be surprised about how and/or for what purposes we are processing their personal information?".

Alternatively, "would our reputation be impacted if our data processing practices made the news tomorrow?"

POPIA prohibits "further processing" which is incompatible or not in accordance with the original purpose of collection. In assessing whether further processing is compatible with the purpose of collection, the organisation would need to consider:

- the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;
- the nature of the information concerned;
- the consequences of the intended further processing for the data subject;
- the manner in which the information has been collected; and
- any contractual rights and obligations between the parties.

Transparency is a key tenet of ethical processing of personal information

In the world of big data analytics, there is a real sense of information inequality. On the one hand there are the organisations who are harnessing big data in a way that they can predict the needs and wants of their customers and on the other hand there are the customers who are too often unaware of how their personal information is collected and what it is being used for.

Section 18 of POPIA aims to close this information chasm by requiring transparency on the part of the responsible party gathering and using the personal information. In this regard, organisations must take reasonably practicable steps to ensure the data subject is aware of, amongst other things, the information being collected (including any indirect sources) and the purpose for which the information is being collected.

There must be at least one lawful basis for processing personal information in terms of POPIA.

Section 11 of POPIA sets out a number of lawful justifications that may apply to the processing of personal information with the most well-known one being that consent was given to such processing. However, there are numerous other justifications including that processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; that

processing complies with an obligation imposed by law; that processing protects a legitimate interest of the data subject; or processing is necessary for pursuing the legitimate interests of the responsible party etc.

Reliance on the correct lawful basis is not always straightforward and will need a thorough assessment having regard to the purposes for which the organisation is processing personal information. This assessment becomes more complex when delving into processing activities involving AI, machine learning, profiling and automated decision making.

There is a general prohibition against certain types of automated decision making...

It would be remiss not to mention that section 71 of POPIA generally prohibits data subjects from being subject to decisions which result in legal consequences for them or which affects them to a substantial degree where that decision is based solely the automated processing of personal information intended to provide a profile of such persons.

One of the exceptions where automated decision making would be allowed is if the decision is governed by a law or code of conduct which incorporates appropriate measures for protecting the legitimate interests of data subjects.

POPIA states that such measures should at a minimum provide an opportunity for a data subject to make representations about a decision and require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information to enable the data subject to make such representations.

When using customer data to develop algorithms, to build models or to automate decisions, ensure human involvement, oversight and governance…

Once data has been ethically collected (in a way that is transparent, and that respects privacy and autonomy), the next principle, applicable to the use of data, is human involvement. When organisations use data to predict whether a customer qualifies for a product eg: home loan, whether they are insurable, or whether their last claim was potentially fraudulent, these decisions cannot be left to algorithms alone. Human involvement and oversight is required. If an algorithm throws up a red flag, human governance is required to understand the basis of the red flag, and to determine whether it is a valid and relevant "red flag". This also allows organisations to correct and improve algorithms that generate false or inappropriate flags.

Those dealing with data and designing data applications in financial institutions should have the requisite ethical competence.

To guard against the ethical harms that can arise from the use of data technologies, as well as the reputational and financial risks that such harms hold for financial institutions, financial institutions must develop the moral sensitivity and ethical judgement of their functionaries, and create environments that support ethical decision-making. Those collecting data, and using data to build models and to develop algorithms, should be sensitive to the ethical dimensions of these technologies, and to its possible downstream uses.

Schalk Engelbrecht
Chief Ethics Officer Risk Management
T: +27 82 713 7656
E: schalk.engelbrecht@kpmg.co.za

Beulah Simpson
Senior Manager KPMG Privacy Practice
T: +27 60 602 3066
E: beulah.simpson@kpmg.co.za

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.