JUTA
POPIA PORTAL

ISSUE 1 • POPIA COMPLIANCE AND CODES OF CONDUCT • MAY 2018

1. OVERVIEW

We discuss what a Code of Conduct is, the purpose of a Code of Conduct, and what specific issues should be regulated under a Code of Conduct.

2. POPIA COMPLIANCE AND CODES OF CONDUCT

In a sense, the POPIA is a bit of an odd bird. In South Africa, we are used to rules-based legislation. Legislation that prohibits things, sets requirements, tells us what to do. This is not the case with the POPIA. As with its European ancestor, the European Union General Data Protection Regulation (the GDPR), the POPIA is based on principles and reasonableness.

Fun fact (ok, maybe just fun for us); the word 'reasonable' appears 44 times in the POPIA.

What does this mean? A 'principle' is a theorem or law that can be applied widely and in many different ways. In fact, to take the concepts of principles and reasonableness a bit further, the POPIA created the concept of a Code of Conduct.

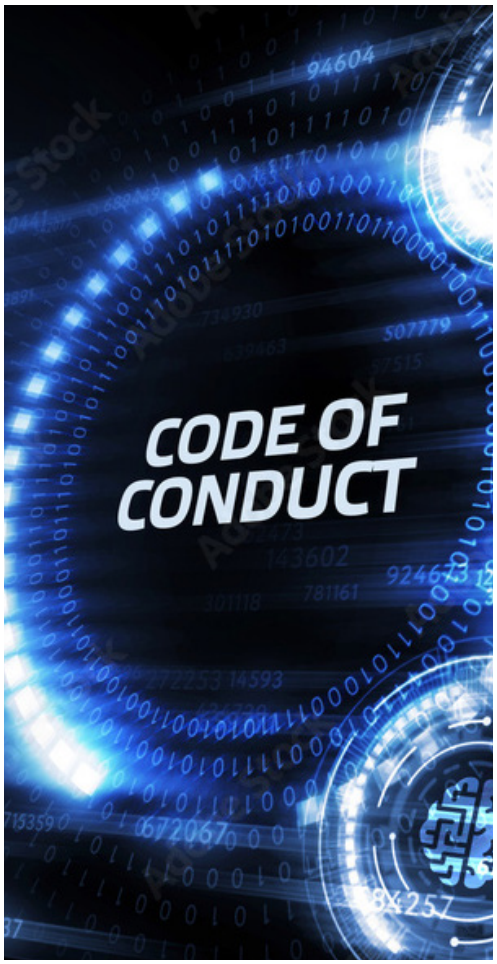
A Code of Conduct can apply to any specified areas such as:

- Information: It is not unusual to find codes of conduct in relation to medical information.
- Bodies: We are currently involved in drafting a Code of Conduct for public universities.
- Activities: Digital marketing comes to mind (thanks Facebook).
- Industries, professions, or vocations: We have heard rumours of a couple of Codes in the making.

Codes of Conduct are used to apply these standards of principles and

2.1. THAT'S NICE, BUT WHAT IS A CODE OF CONDUCT REALLY?

For the POPIA, a Code of Conduct must take the POPIA principles and apply them to the information, activity, or industry that the Code is applicable to. The Code must take the general and translate it into the specific; the principle into guidelines. For instance, the POPIA requires that organisations must be transparent about what information is collected, what it is used for, who it is shared with, etc.



2.2. WHAT ISSUES DOES A CODE OF CONDUCT DEAL WITH?

Specific issues that must be regulated in a Code of Conduct are:

- Information matching programmes: If members of a particular industry are comparing personal information of 10 or more people with that of 10 or more other people in order to produce or verify information, it must be regulated.
- Automated decision making: When significant decisions about a person are made by an algorithm that processes personal information intended to create a profile of a person (e.g., credit worthiness, reliability, location, health, personal preferences, or conduct), it must be regulated.

2.3. WHY SHOULD AN INDUSTRY DEVELOP A CODE OF CONDUCT?

A Code of Conduct can fulfil the following very important functions:

- Optimise how personal information is used.
- Increase the level of protection of privacy and the level of compliance.
- Ensure uniform and sector-appropriate implementation of the POPIA.
- Align the Regulator and the industry's approach to information governance in the industry.

Codes of Conduct can also give the Regulator comfort that a particular industry is committed to become compliant.

2.4. HOW A CODE IS MADE

The Information Regulator can decide to draft a Code on its own or it can be submitted by bodies who are sufficiently representative of the industry the Code will regulate.

The draft Codes then get published for public comment to ensure that all stakeholders who are affected by it have a chance to say their say.

But how do you get to that first draft? Having been in the thick of it, we are reminded of the Otto von Bismarck quote:

'LAWS ARE LIKE SAUSAGES. IT IS BETTER NOT TO SEE THEM BEING MADE.'

It takes a massive amount of stakeholder engagement, research into approaches in other parts of the world in the particular industry, forming working groups to advise in technical areas and, finally, drafting the Code.

2.5. BACK TO PRINCIPLES

To start with it is helpful to agree (with the industry) on guiding principles to make sure that we are still on track throughout the process.

- **The Code is comprised of principles, not rules.** The act incorporates a standard of reasonableness that allows for flexibility to determine if data protection principles have been observed. It also allows you to make a risk versus benefit versus cost analysis when applying the principles. Rules on the other hand are not flexible enough and tend to operate well in some contexts, but unfairly in others.
- **The Code is a clarification of the POPIA.** It must clarify the POPIA principles and must be written in understandable language. We are often guided by the style of the UK ICO codes.
- **The Code must harmonise existing data protection principles in the sector.** Existing guidelines should not be replaced (assuming they are POPIA compliant), they should be absorbed in the Code. No need to reinvent the wheel.
- **The standards set by the Code must be achievable.** If the Code is too difficult to comply with, it will actually increase non-compliance in the industry. Therefore, you must take the cost and impact of compliance into account when drafting the Code. If the average member in the industry cannot become compliant, you should either lower the standards required, or the industry association behind the Code must provide the support and tools to these members to become compliant.