POPIA: DID IT HAPPEN?

SUMMARY

Yes and no.

Many businesses labour under an incorrect impression that midnight, 30 June 2021, something would happen to them if they had not already uploaded a library of often unreadable policies onto their websites and sent mails to everyone they have ever dealt with asking them to consent to a variety of things. Others who were busy with POPIA over the past months think it is over and they can now tick that box as done.

On the 'yes' side

1. Yes, the Act is essentially in full operation from 01 July 2021 onwards. Businesses must employ every effort to show that they are responsibly dealing with the personal information that they work with, whether that information is collected electronically on a website or stored in an office computer, or recorded in a paper application or order form, or otherwise.

2. So many businesses are familiar with sound governance and have always applied common sense safeguards in respect of the data they have in place. For such businesses it is easy to comprehend that POPIA is actually just formalizing a good governance approach and making it obligatory for everyone to do this.

This is good news; and it becomes even better if one considers that today there are indeed many more businesses that are part of this new "information safety" trend than before, due to POPIA.

3. In addition, there is a growing general awareness about safety of personal information and, despite the fact that parts of this 'knowledge' is shaded by misinformation, it is quite a feat that so many South Africans have some awareness of their rights under a piece of national legislation.

If you have not yet done anything, do the following:

1. Identify who is the Information officer. The CEO or head of your business/organisation is the default Information officer.

2. The Information Officer must then:

    a. Do a stock take of the data that the business holds (be it of clients and customers, staff, or third parties that provide services to the business). Don't make it complicated, just start with a list.

    b. Note the "life cycle" of the data: when and how is it collected, used, stored and ultimately deleted (both the physical and electronic records).

    c. Assess whether, in the data "life cycle" in your business, there is at each stage responsible measures in place to ensure that persons who have no reason to have access to the data, can get their hands on it. If you need to make changes, implement that.

    d. Record these steps in a document and share it with your staff so that they know what is happening and why.

Cape Town T: 021 406 9100
Claremont T: 021 673 4700
Fish Hoek T: 021 784 1580
Helderberg T: 021 850 6400
Blouberg T: 021 521 4000
Tyger Valley T: 021 943 3800
Illovo T: 011 219 6200
Fourways T: 010 001 2632
Centurion T: 012 001 1546
Bedfordview T: 011 453 0577
East London T: 043 721 1234

e. Think about when you share information with others (for example a payroll company) and contact them, in writing, to get their undertaking to apply such safeguards as you deem necessary, in respect of all the data that you provided to them in the process of appointing them to render that service.

f. Repeat this process from time to time, because risks change and your business may need to change the way in which you address it.

On the "no" side

1. Nothing dramatic happened overnight!

2. The Information Regulator should have made a more impressive start, at least by ensuring that its portal for the registration of information officers is functioning properly.

3. Direct marketing practices did not overnight disappear or become illegal. It is trickier, for sure, but not banned. On this note, what is and what is not allowed **when you consider electronic communications that businesses use**?

   a. A business may continue to send **information and news** by way of an electronic communication to its existing and new customers that is aligned with the business relationship. There should be an opt-out option in that electronic communication.

   b. A business may continue to send **direct marketing of services or goods** by way of an electronic communication to its existing and new customers that is aligned with the business relationship. There should be an opt-out option in that electronic communication.

   c. If someone is not a customer of that business? The business may send **information and news** without first getting consent from that person. As always, there should be an opt-out option in that electronic communication. The business may however **not** send **direct marketing of services or goods** to that person, unless the business has first asked the person for consent to do so.

   d. In all of this, once a person has asked to opt-out, make sure that your marketing department ensures that such person's details are removed from the names on the marketing list.