THE IMPACT OF POPI ON SOCIAL MEDIA IN SOUTH AFRICA

cerebra

www.cerebra.co.za

In 2009 the South African government first tabled the Protection of Personal Information (POPI) bill in Parliament. The over-arching aim of the bill was to further protect individual's personal information from misuse by companies. This protection covers all instances of information and impacts the way companies engage with customers and collect information on social media platforms.

The **Protection of Personal Information Act 4 of 2013 (POPI)** was published in the Government Gazette in South Africa on the 26th of November 2013. The commencement of the Act is still to be published in a subsequent government gazette publication.

In this article we extract and discuss the elements of the bill that will have an impact on the social media elements of your business and what you may need to change in order to be compliant. We've broken it down into four parts:

1. **The who, what and why**
2. **The detail within POPI**
3. **The effect on social media**
4. **Practical steps to compliance**

PART 1 – THE WHO, WHAT AND WHY

To kick things off you need to get a sense of why POPI has come into existence. Here is an exercise to set the scene:

> *Make a list of all the companies you have a contract with and ones you used to have a contract with. From banks and cell providers to doctors and video stores. Now add to that list all the businesses where you don't have a contract but you still hand over your personal details. Don't forget all the hotels where you've filled in guest cards and competitions you've entered at your local supermarket. Now make a list of all the information these companies have about you. ID number, address, phone numbers, bank details, spouse's details, etc. Now think of what could happen if any single one of those companies didn't protect that information.*

You get the idea. To date there has been no legislation governing how companies should protect that kind of information which means that some take it seriously and others not at all. You know your bank takes it seriously, but your florist probably has as much information.

The South African Constitution already ensures that its citizens have the right to privacy, however, POPI further enhances your ability to protect personal privacy and governs how your personal information is collected and processed by organisations.

Although POPI has yet to be signed into law it aims to:

- Establish how information is collected and processed
- Establish a body (Informational Regulator) to regulate the collection of this information
- Regulate the flow of information across South African borders
- Give rights to South Africans receiving unsolicited information or communication

Who Does POPI apply to?

POPI applies to all South Africans processing personal information, including employers, companies and individuals. That means you, your boss, the company you work for and any business that collects your personal information for any reason what so ever.

POPI now regulates all aspects involved in the processing of personal information from its collection to its destruction. Put simply, if you receive or give any personal information to another party then POPI applies to you. This is a broad net and pretty much includes every business in South Africa.

The question, “why should I care?” is an important one to address. As an individual, any possible exploitation of your personal information should be taken very seriously. At a lower level, having your contact details and location exposed could lead to a barrage of intrusive sales calls. At a higher level, having your credit card number and ID number exposed could lead to identity theft which could cost you everything. Which ever way you look at it, keeping you private information private should be a priority.

As a business that collects information, you will now be required by law to assume the responsibility as the guardian of customer information and do what is required to protect that information. There are both potential legal and brand costs for any company that doesn’t, at the very least, match their customer’s expectations around keeping private information private.

To understand how your business is affected it’s important to understand the scope and definition of ‘personal information’ and ‘processing’:

Personal information includes but not limited to: Race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.

Processing information includes the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as restriction, erasure or destruction of information.

PART 2 - THE NITTY GRITTY

Now that you have the theory we can take a look at the actual bill. POPI contains eight information protection principles for compliance. We've provided a quick look at each of them:

1. Accountability – Step up.

A company is now accountable for overseeing their POPI compliance and is encouraged to appoint an individual within the organisation to oversee this.

2. Processing limitation – Consent and purpose.

Processing of information or sharing of information has to be done under explicit consent from the individual whose information you are processing or sharing. The amount of personal information that is collected from an individual should also not be excessive in relation to the purpose for which it is needed.

3. Purpose specification – What are you doing with the information?

Identifying the purpose for which the personal information is being processed is of utmost importance as it relates directly to how POPI will be applied.

In complying with this principle, organisations are required to:

- Ensure that personal information is only processed for specific, explicitly defined and legitimate reasons that relate to the functions or activities of the organisation
- Take steps to make the data subject aware of the purposes for which the personal information is being collected
- Ensure that personal information is only kept for as long as it is required in order to fulfill the purpose for which it was collected
- Ensure that personal information which you are no longer authorised to retain is deleted or de-identified

4. Further processing limitation – But wait there's more.

Organisations may only use your personal information for the specific, legitimate and explicitly defined purposes for which you gave it to them for. If a magazine collected information for subscriptions, that information cannot then be used for a purpose not pertaining to the subscription to that specific magazine.

5. Information quality – Have any of your details changed?

Organisations are required to ensure that personal information that they process is complete, accurate, not misleading and updated where necessary. Information should be assessed and updated accordingly. Once the information is no longer relevant to its purpose or if the purpose no longer exists, the organisation may no longer process that information.

6. Openness – Who knows what?

Individuals must be aware of what personal information is held by specific entities.

7. Security Safeguards – Am I Safe?

Organisations are required to ensure that all personal information is kept secure. This includes security against the risk of loss, unauthorised access, interference, modification, destruction or disclosure. If any information is compromised the person/s whose information has been compromised should be notified immediately.

8. Data subject participation – What You Say Goes.

After having handed over information to a business you are able to request any changes or deletion. Individuals can access and/or request the correction or deletion of any personal information held about them by an organisation that may be inaccurate, misleading or out of date and the business needs to assist with such requests.

Summary:

1. Accountability – Step up.
2. Processing limitation – Consent and purpose.
3. Purpose specification – What are you doing with the information?
4. Further processing limitation – But wait there's more.
5. Information quality – Have any of your details changed?
6. Openness – Who knows what?
7. Security Safeguards – Am I Safe?
8. Data subject participation – What You Say Goes.

PART 3 - THE EFFECT ON SOCIAL MEDIA

The primary, and most obvious, impact of POPI on your social media activities is that any and all information collected via your social channels will be governed by POPI just like all other customer information. This generally happens when using your social channels as customer service channels and you ask customers for their contact details, ID or customer numbers via private messaging. All of this information is governed by POPI.

Should you use an agency to run your social media (we know a great one), they are operating as a third party on your behalf. As such, they would be collecting and processing on your behalf, or at the least, they would have access to view and capture customer information. The agency would be required to conform to the POPI requirements on your behalf.

You, or your agency, should also ensure that your actions are not endangering the private information of your customers. As an example, asking someone to direct message you on Twitter runs the risk that they reply publicly, thus exposing their information. This happens more often that you think. A solution could be for you to initiate the direct message contact, and they can simply reply privately.

Another big impact of POPI on social media deals with the development on influencer lists. An influencer list is a list of people who are influential on various levels on social media. They may be customers, bloggers or simply people who have a large, influential reach. Many of the people on these lists are not journalists so their information is 'less public'. If you have an influencer list then that set of private information will be governed by POPI. Be aware that when you first collected an influencer's information it would have been for a specific purpose (an event invite). That influencers info gets added to the list but doesn't mean that it can be shared with other clients for a different purpose.

POPI also serves as a general warning to all South Africans. POPI only protects your private information, as such, any information that you share publicly will automatically fall outside of this Act's protection. If you list your email address or telephone number on your Facebook page, and that information is publicly available, then it's free for companies to collect and use. You can't then claim protection under POPI if this information gets used. All social media users should be highly aware of what information you have offered up publicly.

PART 4 - PRACTICAL STEPS TO COMPLIANCE

There is a grace period of one year for South African businesses to comply with POPI. Under special circumstances, this can be extended to a maximum of three years, but don't think that laziness is a special circumstance.

Non-compliance with POPI could lead to penalty of a fine and/or imprisonment of up to twelve months for those in charge of compliance within an organisation. POPI is a far-reaching piece of legislation that is likely to affect most South African businesses and individuals in some way or other. In order to safeguard against penalties, businesses will need to act quickly in determining the affect POPI will have and take the appropriate steps to become compliant.

Here are a few practical steps to follow to ensure your social media activities are compliant:

1. Evaluate your social data capturing techniques and ensure the capture, storage and use of the data complies with your overall company POPI governance.
2. Work with your agency to ensure that your services contract covers the legal POPI requirements of a third party company.
3. Ensure that your company's risk officer (or whoever is responsible for POPI compliance) understands your social objectives and understands how social conforms to POPI.
4. Review your influencer lists and ensure you know:
    - which information is in the public domain and can be used 'freely'
    - where and how you got the information
    - what the purpose of original collection was
    - that you have permission to use the information
    - You may be required to re-collect information and obtain consent for future use for a broad purpose.
5. Ensure there are processes to deal with the Regulator, complaints and security breaches

ABOUT CEREBRA:

Cerebra was founded by Mike Stopforth (www.mikestopforth.com) in 2006. Since then, the integrated strategic communication agency has grown from a small consulting outfit to a large team of incredibly talented, hard-working personalities who all share in a passion for effective communication. It's this passion and our learnings, which we hoped to share with you in this guide.

We are in the business of aiding companies in building communities, engaging with these communities and finally activating these communities through the appropriate communication channels, whether traditional or social media.

For more visit www.cerebra.co.za

ABOUT CONCILLIUM LEGAL SERVICES:

Concillium Legal Services provides legal consulting and advisory services on a outsourced basis, without the burden of employing permanent legal resources or the expense of briefing a law firm.

Concillium provides intellectual capital that spans across a wide range of industries, which enables us to assist you with your unique business challenges and other strategic issues that require legal input.

CONSILIUM
LEGAL SERVICES (PTY) LTD

cerebra
www.cerebra.co.za