usercentrics

Checklist for the Protection of Personal Information Act (POPIA) for South Africa

September 2021

DISCLAIMER

These statements do not constitute legal advice. They merely serve to support and inform you about the current legal situation. Please consult a qualified lawyer should you have any legal questions.

POPIA Checklist

If your company has customers in South Africa, or plans expansion there, and you collect or process personal data, you need to comply with the Protection of Personal Information Act (POPIA).

POPIA received Presidential assent in November 2013. Sections of POPIA coming into effect have been staggered in the years since, with key remaining sections coming into effect on July 1st, 2020. Organizations had 12 months from that date to enact POPIA compliance requirements, and enforcement began as of July 1st, 2021.

The good news is: if you are already compliant with the GDPR or LGPD, then you have already done a great deal of the work necessary to comply with POPIA.

To help you achieve POPIA compliance, follow these steps:

Steps	Roadmap
1. Identify if your organization needs to comply	• Your business processes the **personal data of people in South Africa**, regardless of where your business is located.
2. Create a comprehensive Privacy Policy	• Ensure it is easy to f**ind, read and understand** for the average user. • **Inform** about who has access to personal data collected (e.g. from cookies). • **Implementation**: make the information and consent preferences about data processing available in a **Privacy Banner** when users visit your site. A **Consent Management Platform** ensures that you can include all necessary information and obtain required consents.
3. Inform users about their rights	• Inform users about the **nine fundamental rights** that data subjects have under **Section 5** of POPIA e.g. right to **erasure**, right to be **informed**, and right to **object**.

Steps	Roadmap

4. Inform users that you use cookies or other tracking technologies	• Ensure that you **inform users of your intentions** at or before the point you start collecting data.
	• Particularly inform users about:
	  ○ The specific purpose of the processing;
	  ○ The type and duration of the processing;
	  ○ The identity of the responsible party and their contact information;
	  ○ The shared use of data by the responsible party, and the purpose;
	  ○ The responsibilities of the agents that will carry out the processing;
	  ○ The data subject's rights, with explicit mention of the rights listed in **Section 5** of POPIA.
	• Include this information in your **Privacy Policy**.

5. Explain in the first layer of the privacy banner what your cookies or other web technologies are doing and why	• Inform users about the **purpose of each cookie or web technology separately** to ensure you obtain specific and granular consent for each cookie objective. Users must have the option to **grant or withdraw consent for each purpose.** • It should be stated in the **first layer of the Privacy Banner**.

Steps	Roadmap
6. **Obtain users' voluntary and informed consent to store cookies on their device(s) and enable refusal of consent or adjustment of preferences in the future**	• Necessary where cookies involve the **collection and processing of personal data** from users (e.g. if the information can be linked to a particular individual's identity). • **Consent must be freely given**: Equal presentation and accessibility of "Accept" and "Reject" buttons. Refusing consent must be an equally accessible option. • **Consent must be easy to withdraw**: in the second layer users have to have the option to withdraw their consent. • **Documented**: You have the burden of proof of consent in the case of an audit.
7. **Collect and process data only after obtaining valid consent**	• Ensure that **no cookies are loaded until users have given consent**. • Once valid consent has been obtained, you can collect and process personal data for the purposes for which you informed users (i.e. using the web technologies to which they consented).
8. **Document and store consent received from users**	• Comply with documentation obligations to ensure you can verify users' consent in case of complaint or audit by South African data protection authorities.
9. **After opt out, ensure that no further data is collected or forwarded**	• Ensure that from the **moment of the objection** on, no further data is collected or forwarded. This includes declined consent for new users or updated consent preferences for existing users.

POPIA Checklist

POPIA Cookie Requirements

Cookies covered by POPIA

Identifiable data is protected by POPIA. Thus, **cookies and other tracking web technologies** – that collect data that can be associated with a natural person – are subject to privacy compliance obligations under the law. E.g. the information is linked or linkable to a particular user, IP address, device or other specific identifier.

The **exception is anonymized or permanently de-identified data** under Section 6, which is not considered personal data under POPIA.

Lawful Processing

Section 4 of POPIA outlines provisions for the parameters of restrictions on personal data collection and processing, how the Act applies to different population groups, and who is responsible for monitoring and enforcement.

For violations, POPIA has provisions for both monetary and carceral penalties. The maximum fine is ZAR 10 million (approx. EUR 500,000) and the maximum prison sentence is 10 years for certain responsible individuals and certain violations.

Requirements for POPIA (South Africa)	Is Usercentrics compliant?
Freely given and informed consent is necessary	✔
The purpose has to be provided (first layer of the privacy banner)	✔
The recipient has to be named (second layer of the privacy banner)	✔
Withdrawal of consent has to be possible (second layer of the privacy banner)	✔
Options to grant or decline consent must be equal	✔
Proof that consent has been given must be stored	✔
The option to give or withdraw granular consent for each data processing purpose has to be provided	✔