An In-Depth Look at South Africa's Protection of Personal Information Act (POPIA) and Its Comparison with GDPR

Disclaimer: This publication is intended to provide a general overview and analysis of data protection laws and is not intended to serve as legal advice or guidance. While every effort has been made to ensure the accuracy of the information contained in this publication, the author does not guarantee its completeness or correctness.

The information provided in this publication is subject to change and may not reflect the most current legal developments. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules, and regulations, there may be omissions or inaccuracies in the information contained in this publication.

This publication is provided with the understanding that the author is not herein engaged in rendering legal, accounting, tax, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional legal, tax, accounting, or other competent advisers.

Before making any decision or taking any action, you should consult a professional. The author is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this publication is provided "as is", with no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this information, and without warranty of any kind, express or implied.

In no event will the author be liable to you or anyone else for any decision made or action taken in reliance on the information in this publication or for any consequential, special, or similar damages, even if advised of the possibility of such damages. Use of this publication is at your own risk.

Abstract

This comprehensive review discusses South Africa's Protection of Personal Information Act (POPIA) and its similarities and differences with the European Union's General Data Protection Regulation (GDPR). POPIA, a privacy law enacted in 2013 and effective from July 2020, sets stringent conditions for the lawful processing of personal information by organizations. These include obtaining individual consent, maintaining data accuracy, and ensuring data security. Non-compliance can result in hefty fines.

While POPIA and GDPR share many principles, notable differences lie in their jurisdiction, consent requirements, age of consent for children, the necessity of a Data Protection Officer, timelines for data breach reporting, the 'right to be forgotten', penalties, and provisions for cross-border data transfers.

The article also elaborates on specific sections of POPIA applicable to organizations processing personal information, including sections detailing the law's application and interpretation, the conditions for the lawful processing of data, the rights of data subjects, and conditions for transferring personal data to foreign countries. It underscores the need for expert consultation for compliance with these complex regulations.

Overview

South Africa's Protection of Personal Information Act (POPIA) is a law that regulates the processing of personal information by organizations in South Africa. The Act was passed in 2013 and came into effect on July 1, 2020. POPIA is similar to the European Union's General Data Protection Regulation (GDPR) in many respects, but there are also some key differences.

Under POPIA, organizations that process personal information must comply with a number of requirements, including:

- Obtaining consent from individuals before collecting or processing their personal information.
- Limiting the collection and processing of personal information to what is necessary for a specific purpose.
- Keeping personal information accurate and up to date.
- Protecting personal information from unauthorized access, use, disclosure, or destruction
- Providing individuals with access to their personal information and the right to have it corrected or deleted.

Organizations that fail to comply with POPIA may be subject to fines of up to ZAR10 million (approximately USD 640,000).

Here are some of the key provisions of POPIA:

- Purpose limitation: Personal information may only be collected and processed for a specific purpose that is known to the individual and may not be used for any other purpose without the individual's consent.
- Consent: Individuals must give their consent before their personal information can be collected or processed. Consent must be freely given, specific, informed, and unambiguous.
- Data minimization: Personal information must be collected and processed only to the extent that is necessary for the purpose for which it is being collected or processed.
- Accuracy: Personal information must be accurate and up to date.
- Security: Personal information must be protected from unauthorized access, use, disclosure, or destruction.
- Individuals' rights: Individuals have the right to access their personal information, to have it corrected or deleted, and to object to its processing.
- Enforcement: The Information Regulator is responsible for enforcing POPIA. The Regulator may impose administrative penalties on organizations that fail to comply with the Act.

POPIA is a comprehensive law that sets out a number of requirements for organizations that process personal information. Organizations that fail to comply with POPIA may be subject to significant penalties.

DATA PROTECTION MATTERS

Key Differences between POPIA & GDPR

The Protection of Personal Information Act (POPIA) and the General Data Protection Regulation (GDPR) are two distinct legal frameworks regulating the processing of personal information, enacted by South Africa and the European Union respectively. While they share many similarities, there are also key differences:

Jurisdiction: GDPR applies to any organization, irrespective of its location, if it processes the personal data of EU citizens or residents. POPIA, on the other hand, applies to organizations processing personal data within South Africa or if the organization is based in South Africa and processes data elsewhere.

Consent: Under GDPR, consent must be explicit, freely given, informed, and unambiguous for each specific purpose. POPIA also requires consent but allows for personal data processing under a wider range of circumstances such as if the processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party.

Children's consent: GDPR requires parental consent for processing the personal data of children under 16 (Member States can lower the age to 13). POPIA does not specify a similar age requirement, but it provides extra protection for children's personal information.

Data Protection Officer (DPO): GDPR requires the appointment of a DPO in certain circumstances, such as for public authorities or when large-scale systematic monitoring of individuals is taking place. POPIA does not explicitly require a DPO but does mandate the appointment of an Information Officer who is responsible for encouraging compliance with POPIA within an organization.

Data breaches: Both regulations require data breaches to be reported, but the timelines differ. GDPR mandates reporting a breach to the supervisory authority within 72 hours, whereas POPIA requires the breach to be reported "as soon as reasonably possible."

Right to be forgotten: GDPR provides the explicit "right to be forgotten," allowing data subjects to have personal data erased in certain circumstances. While POPIA provides a data subject the right to request a responsible party to correct, delete, or destroy personal information, it does not explicitly contain the "right to be forgotten."

Fines and Penalties: GDPR can impose fines up to €20 million or 4% of a firm's total global turnover, whichever is higher. POPIA, on the other hand, can impose penalties of a fine and/or imprisonment of up to 10 years, or in certain cases, an unlimited administrative fine.

Cross-Border Transfers: Both regulations allow for the transfer of personal data outside their respective regions, but the requirements differ. GDPR requires an "adequacy decision," "appropriate safeguards" such as Standard Contractual Clauses, or in some cases explicit consent. POPIA also allows for cross-border transfers but requires that the recipient country has laws, binding corporate rules, or binding agreements that offer an adequate level of data protection.

A Condensed Overview of Sections Relevant to organizations holding Personal Information

Section 3 details the application and interpretation of the Act related to the processing of personal information:

1) The Act applies to the processing of personal information that is entered in a record by or for a responsible party. This can be done through automated or non-automated means, provided that when the information is processed by non-automated means, it forms part of a filing system or is intended to form part of one. The Act applies whether the responsible party is domiciled in the Republic or not, as long as they use automated or non-automated means in the Republic. The only exception is when these means are used solely to forward personal information through the Republic.

2) This Act applies, with some exceptions, to the exclusion of any other legislation that regulates the processing of personal information if that legislation is materially inconsistent with an object, or a specific provision, of this Act.

3) If other legislation sets out conditions for the lawful processing of personal information that are more extensive than those in Chapter 3 of this Act, then those extensive conditions prevail.

4) The Act must be interpreted in a way that:

- gives effect to the purpose of the Act set out in Section 2;

- does not prevent any public or private body from exercising or performing its powers, duties, and functions in terms of the law, as long as such powers, duties, and functions related to the processing of personal information and such processing is in accordance with this Act or any other legislation that regulates the processing of personal information.

5) For the purposes of this section, "automated means" refers to any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

Section 4 outlines the conditions for the lawful processing of personal information:

1) There are eight conditions for the lawful processing of personal information by or for a responsible party, which include: Accountability (section 8), Processing Limitation (sections 9 to 12), Purpose Specification (sections 13 and 14), Further Processing Limitation (section 15), Information Quality (section 16), Openness (sections 17 and 18), Security Safeguards (sections 19 to 22), and Data Subject Participation (sections 23 to 25).

2) These conditions are not applicable to the processing of personal information if such processing is excluded from the operation of this Act under sections 6 or 7, or exempted from one or more of the concerned conditions in relation to such processing under sections 37 or 38.

3) The processing of special personal information is prohibited unless the provisions of sections 27 to 33 apply, or the Regulator has granted authorization under section 27(2). If such authorization has been granted, the conditions for lawful processing of personal information as referred to in Chapter 3 must be complied with, subject to sections 37 or 38.

4) The processing of personal information of a child is also prohibited unless the provisions of section 35(1) apply, or the Regulator has granted authorization under section 35(2). In these cases, the conditions for lawful processing of personal information as referred to in Chapter 3 must be complied with, subject to section 37.

5) The processing of special personal information of a child is prohibited unless the provisions of sections 27 and 35 apply. In these cases, the conditions for lawful processing of personal information as referred to in Chapter 3 must be complied with, subject to section 37.

6) The conditions for the lawful processing of personal information for the purpose of direct marketing are reflected in Chapter 3, read with section 69 as far as that section relates to direct marketing by means of unsolicited electronic communications.

7) Sections 60 to 68 provide for the development of codes of conduct, in appropriate circumstances, to clarify how the conditions referred to in subsection (1) are to be applied or complied with within a particular sector, subject to any exemptions that may have been granted under section 37.

Section 5 outlines the rights of data subjects (individuals whose personal information is being processed):

1) Data subjects have the right to have their personal information processed lawfully, in line with the conditions set out in Chapter 3.

2) They have the right to be notified when:

- their personal information is being collected (as per section 18),

- their personal information has been accessed or acquired by an unauthorized person (as per section 22).

3) They have the right to verify if a responsible party holds their personal information and to request access to their personal information (as per section 23).

4) They have the right to request, when necessary, the correction, destruction, or deletion of their personal information (as per section 24).

5) They have the right to object, on reasonable grounds relating to their particular situation, to the processing of their personal information (as per section 11(3)(a)).

6) They have the right to object to the processing of their personal information for purposes of direct marketing at any time (as per section 11(3)(b) or section 69(3)(c)).

7) They have the right not to have their personal information processed for direct marketing purposes by means of unsolicited electronic communications, except as referred to in section 69(1).

8) They have the right not to be subject, under certain circumstances, to a decision based solely on automated processing of their personal information intended to provide a profile of them (as per section 71).

9) They have the right to submit a complaint to the Regulator about alleged interference with the protection of personal information or in respect of a determination of an adjudicator (as per section 74).

10) They have the right to institute civil proceedings regarding alleged interference with the protection of their personal information (as per section 99).

Section 72 outlines the conditions for transferring personal information about a data subject from the Republic to a third party in a foreign country:

1) A responsible party within the Republic cannot transfer personal information to a third party in a foreign country unless:

- The foreign recipient is subject to a law, binding corporate rules or a binding agreement that effectively upholds principles for reasonable processing of the information. These principles should be substantially similar to the conditions for lawful processing of personal information relating to a natural person (and, where applicable, a juristic person) and should include provisions relating to further transfer of personal information from the recipient to third parties in a foreign country.

- The data subject consents to the transfer.

- The transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures in response to the data subject's request.

- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party.

- The transfer is for the benefit of the data subject, it is not reasonably practicable to obtain the data subject's consent to the transfer, and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

2) In this section, "binding corporate rules" are defined as personal information processing policies within a group of undertakings adhered to by a responsible party or operator when transferring personal information to a responsible party or operator within that same group in a foreign country. A "group of undertakings" refers to a controlling undertaking and its controlled undertakings.