iab south africa

A Practical Guide to Data Protection for the Digital Advertising Industry in South Africa

2021

Prepared by the IAB South Africa

Visit iabsa.net

TABLE OF CONTENTS

ACRONYMS

DPA	Data Protection Authority
EU	European Union
IAB	Interactive Advertising Bureau
ICO	Information Commissioner's Office
GDPR	General Data Protection Regulation 2016/679
PAIA	Promotion of Access to Information Act 2 of 2000
POPIA	Protection of Personal Information Act 4 of 2013
UK ICO	United Kingdom Information Commissioner's Office

FOREWORD

The IAB South Africa is pleased to launch ***A Practical Guide to Data Protection for the Digital Advertising Industry in South Africa***. This resource is intended to assist our members, as well as the advertising industry more broadly, to ensure legal compliance with relevant data protection frameworks, to safeguard the rights of data subjects, and to enable organisations to continue to process information in a reasonable and responsible manner.

The Interactive Advertising Bureau (IAB) South Africa empowers the media and marketing industries to thrive in the digital economy. Its membership is comprised of more than 150 leading media companies, brands, and the technology firms responsible for enabling excellence in digital marketing focusing on identifying and targeting audiences, delivering, and optimising campaigns to these audiences and the innovation and selling of such activities. The non-profit, non-government, trade group fields critical research on interactive advertising, while also educating brands, agencies, publishers. and the wider business community on the importance of digital marketing.

The IAB Global Network brings together 45 national IABs and three regional IABs to share challenges, develop global solutions and advance the digital advertising industry worldwide. IABs are located in North America, South America, Africa, Asia, Asia Pacific, and Europe. Each association is independently owned and operated, functioning under bylaws consonant with local market needs.

In this regard, we recognise the importance of the data-driven era that the digital age presents. This has presented innumerable opportunities for organisations to engage with the public, enhance their service offerings and interact with persons who might otherwise have been excluded. However, in doing so, there is a constitutional imperative to respect the privacy rights of the persons with whom we engage.

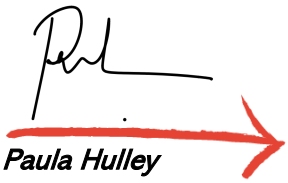
It is for this reason that the IAB South Africa, in line with our mandate from the IAB globally, has prioritised the need to support our members with data protection compliance, approaching it from a rights-based lens that is duly cognisant of our commitment to the Constitution of the Republic of South Africa, 1996 and other relevant legal frameworks, such as the Protection of Personal Information Act 4 of 2013 and the Promotion of Access to Information Act 2 of 2000. In particular, we seek to support our members in grappling with the implementation of data protection laws in a practical and effective manner.

The launch of this guide is only one step in the IAB South Africa's broader strategy. Additionally, we offer training workshops on data protection compliance for the advertising industry, publish advisory notes for our members, and have been engaging on the Transparency and Consent Framework pioneered by the IAB Europe. Through these measures, we hope to contribute to making the current regulatory landscape easier to navigate and assist our members to respond to the changes that these laws herald for the industry.

While data protection laws may disrupt some of the ways in which the industry operates, we also see a marked increase in members of the public demanding agency over their personal information, including how it is being used, with whom it is being shared and how securely it is

being stored. This is therefore an opportune time for the advertising industry to step up and show its commitment to respecting and protecting personal information, to assist the public to make informed decisions, and to boost trust in our industry.

For any queries or to learn more about the IAB South Africa, please visit www.iabsa.net.



Paula Hulley
CEO, IAB South Africa

Importance of Data Protection Compliance

Every day, we create and give away information about ourselves, whether this is through the completion of a form, an online search, posting on social media or reading the news on the internet. Some of this information may be voluntarily provided, while other information may be automatically recorded. This information may seem small and inconsequential when viewed in isolation but may be collated to create a larger image of where we have been, what we like and what views we hold.[1]

In recognition of the risks that this presents, there has been a significant increase in data protection laws being enacted across the globe. Such laws seek to give effect to the right to privacy, and to ensure the security of individuals' personal information by regulating the collection, use, transfer, and disclosure of such information. Compliance with such laws is an important part of running a business successfully, as it gives customers the assurance that their personal information is being processed securely and responsibly.

There are many reasons why data protection compliance is important for organisations: it helps to reduce the number of data breaches that an organisation may suffer; it helps to prevent loss of revenue; it protects customers' privacy; it can maintain and improve brand value; it supports an organisation's code of ethics; and it may give a competitive advantage over other businesses.[2] It also serves to maintain public, investor and customer trust, and to build customer loyalty.[3]

While, for many, it is a necessary regulatory compliance exercise that must be undertaken – which indeed it is – it is also about meaningfully realising the right to privacy in the digital era, which is inextricably linked to human dignity, equality, and autonomy of the person, and deserving of being appropriately safeguarded.[4]

This guide unpacks the legislative requirements of the Protection of Personal Information Act 4 of 2013 (POPIA) and provides several implementation steps to guide the compliance process. The implementation of POPIA will differ depending on the size and operations of each organisation and we encourage finding tailored approaches which allow for the processing of personal information in a way which gives effect to the constitutional rights to privacy and access to information and is legally compliant.

[1] ALT Advisory, 'Bits of you', 2021: https://altadvisory.africa/wp-content/uploads/2021/01/Bits-of-you.pdf.
[2] EC-Council, 'The importance of data security and privacy for businesses', 2020: https://blog.eccouncil.org/the-importance-of-data-security-and-privacy-for-businesses/.
[3] CPO Magazine, 'Twelve reasons why data privacy protection bring business value', 2018: https://www.cpomagazine.com/blogs/privacy-intelligence/12-reasons-why-data-privacy-protection-brings-business-value/.
[4] ALT Advisory, 'Why POPIA is about rights – not just compliance', 2020: https://altadvisory.africa/2020/06/23/why-popia-is-about-rights-not-just-compliance/.

Disclaimer

While all reasonable steps have taken by the IAB South Africa to ensure the accuracy of the information contained in this guide, regulatory compliance processes will be unique to each individual organisation. The IAB South Africa, therefore, encourages organisations to engage data protection professionals to complement their regulatory compliance processes and to ensure that matters unique to an individual organisation are fully considered. The IAB South Africa is not responsible for any errors or omissions, or for the results obtained from the use of the information contained in this guide.

Complaints

To the extent that organisations may become aware of non-POPIA compliant data protection practices, complaints can be directed to:

The Information Regulator of South Africa
complaints.IR@justice.gov.za

OVERVIEW OF THE LEGAL FRAMEWORK

In this section we briefly discuss the rights to privacy and access to information enshrined in the Constitution, and the legislation which was enacted to give effect to these rights – POPIA and PAIA.

Constitutional Framework

South Africa is founded on the values of human dignity, the achievement of equality and the advancement of human rights and freedoms.[5] The Constitution,[6] as the supreme law of South Africa,[7] imposes an obligation on the state to respect, protect, promote and fulfil the rights in the Bill of Rights. The Bill of Rights binds all organs of state,[8] as well as natural and juristic persons to the extent applicable.[9]

The following rights, provided for in the Bill of Rights, underpin the legislative framework applicable to data protection:

The Right to Privacy

Section 14 of the Constitution provides for the right to privacy which states:

"Everyone has the right to privacy, which includes the right not to have –
a) their person or home searched;
b) their property searched;
c) their possessions seized; or
d) the privacy of their communications infringed.

Although data protection and personal information are not specified in the text of section 14, it has been recognised that the right to privacy includes the ability of an individual to determine what information about themselves is made public, and to control how that information is collected and used. The right accordingly includes the right to protection against the unlawful collection, retention, dissemination and use of personal information.[10]

The right is recognised in article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. The United Nations High Commissioner for Human Rights, has remarked on the right to privacy in the context of personal information:[11]

> "The right to privacy is not only impacted by the examination or use of information bout a person by a human or an algorithm. Even the mere generation and collection of data

[5] Section 1(a) of the Constitution.
[6] The Constitution of the Republic of South Africa, 1996.
[7] Section 2 of The Constitution.
[8] Section 8(1) of the Constitution.
[9] Section 8(2) of the Constitution.
[10] Preamble of POPIA.
[11] United Nations General Assembly, Report of the United Nations High Commissioner for Human Rights 'The Right to Privacy in the Digital Age' 3 August 2018 [available at: https://undocs.org/A/HRC/39/29].

relating to a person's identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk."

The Right to Access Information

Section 32 of the Constitution provides for the right to access to information which states:

1. "Everyone has the right of access to
    a. any information held by the state; and
    b. any information that is held by another person and that is required for the exercise or protection of any rights.
2. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

The right of access to information gives meaning to the constitutional values of accountability, responsiveness and openness, and enables the public to seek transparency from both public and private sector actors. It is both an important right in itself, as well as an enabler of the full range of fundamental rights.

The right is recognised in article 19 of the Universal Declaration of Human Rights and in article 19 of the International Covenant on Civil and Political Rights. The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has noted that:[12]

> "information-rich environments help promote good decision-making and meaningful pubic-debate."

Legislative Framework

Overview of the Protection of Personal Information Act 4 of 2013

POPIA is the comprehensive data protection legislation enacted in South Africa. It aims to give effect to the constitutional right to privacy, whilst balancing it against competing rights and interests, particularly the right of access to information.

POPIA was signed into law on 19 November 2013 and has come into force incrementally.[13] Section 114 of POPIA, which came into force on 1 July 2020, requires compliance with POPIA within one year from the date of its commencement. Accordingly, all responsible parties will be required to have compliance measures in place by 30 June 2021.

[12] United Nations General Assembly 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression.' 18 August 2017 [available at: https://undocs.org/A/72/350].
[13] In accordance with Proclamation No. R25 of 2014 the following sections came into force with effect from 11 April 2014: section 1; Part A of chapter 5; section 112 and section 113. In accordance with Proclamation No. R21 of 2020, the following sections came into force with effect from 1 July 2020: sections 2 – 38; sections 55 – 109; section 111 and section 114(1), (2) and (3); and the following sections came into force with effect from 30 June 2021: sections 110 and 114(4).

POPIA sets out the conditions for the lawful processing of personal information and establishes the Information Regulator – an independent body which is empowered to monitor and enforce compliance by public and private bodies with PAIA and POPIA. It further notes the penalties for non-compliance and empowers the Information Regulator to draft Regulations.

The Information Regulator has published the Regulations Relating to the Protection of Personal Information, 2018 (the Regulations)[14], which provide for, among other things, the completion of a data protection impact assessment, the forms to be used in respect of complaints, and further detail on the responsibility of Information Officers. The Regulations will come into force incrementally.[15] Importantly, the Regulations provide Form 4 which must be used by a responsible party who wishes to process personal information for the purposes of direct marketing by electronic communication.[16]

Draft Guidelines on the Registration of Information Officers, 2020 (the Draft Guidelines)[17] have also been developed by the Information Regulator. The Draft Guidelines provide further detail on the designation and responsibilities of Information Officers.

Overview of the Promotion of Access to Information Act 2 of 2000

The Promotion of Access to Information Act 2 of 2000 (PAIA) was enacted to give effect to the constitutional right of access to information. It regulates the process to access any information held by the state or by any other person which is required for the exercise or protection of any right. The purpose of PAIA is to foster a culture of transparency and accountability in public and private bodies and to actively promote a society in which people have effective access to information.

PAIA regulates the manner in which requests for access to information must be made, as well as the lawful grounds of refusal of access. Prescribed templates for requests for access to information have been developed for public[18] and private bodies.[19]

The Information Regulator, established in POPIA, is empowered to monitor and enforce compliance by public and private bodies with PAIA.

Importantly, section 51 of PAIA places an obligation on private bodies to compile an access to information manual. The Regulations ascribe this responsibility to the Information Officer who must develop, monitor and maintain the manual.

[14] The Regulations may be accessed here: https://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister.pdf
[15] Regulation 4 will be effective on 1 May 2021; Regulation 5 will be effective on 1 March 2021; and the residual regulations will be effective from 1 July 2021.
[16] A template of this form is provided for in Annexure B.
[17] The Draft Guidelines may be accessed here: https://www.justice.gov.za/inforeg/docs/InfoRegSA-Guidelines-InfoOfficers-Invite-20200717.pdf
[18] Form A can be accessed here: https://www.justice.gov.za/forms/paia/J750_paia_Form%20A.pdf
[19] Form C can be accessed here: https://www.justice.gov.za/forms/paia/J752_paia_Form%20C.pdf

APPLICATION OF POPIA

POPIA applies to the processing of personal information of a data subject, which has been entered into a record by or for a responsible party.

The definitions are set out in section 1 of POPIA. The relevant role-players and key definitions are outlined below.

Key Role Players in terms of POPIA

- The "***data subject***" is the person to whom the personal information relates. For example, if you collect and store the CVs of prospective and current employees, the employees would be considered the data subjects.

- The "***responsible party***" is the public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

- The "***operator***" is a person or body which processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, if a third-party company is contracted to manage your employees' tax then they would be considered an operator, because they process personal information on your behalf.

- The "***Information Officer"*** refers to an individual who works within a private or public body and has been designated, in compliance with section 56 of POPIA, to be responsible for ensuring compliance with POPIA.

- The "***Information Regulator"*** is an independent body established by POPIA which is mandated to enforce compliance with POPIA.

Relevant Definitions

The following definitions are also of relevance:

- The term "***personal information***" is defined to mean:

  "information relating to an identifiable, living, natural person, and where its applicable, an identifiable, existing juristic person, including but not limited to–

  (a) information relating to the 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;

  (b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person.

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or of the disclosure of the name itself would reveal information about the person".

- The term "***processing***" is defined to mean:

  "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

  (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

  (b) dissemination by means of transmission, distribution or making available in any other form; or

  (c) merging, linking, as well as restriction, degradation, erasure or destruction of information".

- The term "***special personal information***" includes information relating to a data subject's religious or philosophical beliefs; race or ethnic origin; trade union and political affiliations; biometric information; information relating to their health and sex life; as well as information relating to criminal conduct.

Scope of Application

Section 3(1) of POPIA details the scope of application of the Act and must be read with sections 6, 7 and 37 which detail the exclusions. All private and public bodies who process personal information must comply with POPIA. This includes members of the public, partnerships and companies which process personal information for the purpose of business. It also includes government departments, as well as any institution which exercises a public power or performs a public function. It also applies to non-governmental organisations and civil society organisations. In sum, all natural and juristic persons must comply with POPIA, unless the processing of personal information falls within one of the exclusions. The Application of the act is dealt with in detail below.

Application and interpretation of the Act

3.(1) This Act applies to the processing of personal information –

a) Entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and

b) Where the responsible party is –

i. Domiciled in the Republic; or

i. Not domiciled in the Republic, but makes use of automated or non-automated means in the Republic; unless those means are used only to forward personal information through the Republic.

In terms of the above, POPIA will apply when the following considerations are met:

Consideration	Important Definitions
1. ***Processing of personal information:*** **there must be processing of personal information.**	**Processing** includes any operation or activity concerning personal information, some of which include: collection, recording, organisation, collation, retrieval, and use. The listed activities constitute 'processing' regardless of whether they are done automatically or not. **Personal Information** means information relating to an identifiable, living, natural person, and an identifiable existing juristic person. POPIA does not restrict its scope of application to South African citizens. Rather, POPIA protects the personal information of all data subjects in South Africa, provided that the data subject's personal information is processed by a responsible party who falls within the scope of application of POPIA.
2. ***Entry into a record:*** **the personal information must be entered into a record by or for a responsible party.**	**Record** means any recorded information, regardless of form or medium. This includes writing on any material and information produced, recorded, or stored by means of computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information.

		Responsible party means a public or private body which alone or in conjunction with others, determines the purpose of and means for processing personal information.
3.	***Automated or non-automated means:*** **it is irrelevant whether the responsible party makes use of automated or non-automated means. If the personal information is processed by non-automated means, this must form part of a filing system or be intended to form part thereof for POPIA to apply.**	**Automated means** is defined as any equipment capable of operating automatically in response to instructions given for the purpose of processing information.
4.	***Domiciled in South Africa:*** **it is irrelevant whether the responsible party is domiciled in South Africa, provided that the responsible party makes use of automated or non-automated means in South Africa. POPIA does not apply if those means are only used to forward personal information through South Africa.**	POPIA applies to all responsible parties domiciled in South Africa. A domicile refers to the place which is considered to be a person's permanent residence. For companies, this means that the company was incorporated, established or formed in South Africa.

The Exclusions

POPIA provides for certain exclusions from its scope of application. The exclusions include the following:

- ***Personal or household activity:*** processing of personal information in the course of a purely personal or household activity.

- ***De-identification of personal information:*** personal information that has been de-identified to the extent that it cannot be re-identified again, even when combined with other publicly available datasets. The de-identification of personal information means to delete any information that identifies the data subject; can be used or manipulated by a reasonably foreseeable method to identify the data subject; or can be linked by a reasonably foreseeable method to other information that identifies the data subject.

- ***National security:*** processing of personal information by or on behalf of a public body which involves national security. This exclusion only applies to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

- ***Law enforcement:*** processing of personal information by or on behalf of a public body, the purpose of which is the prevention, detection, investigation or proof of offences, the prosecution of offenders; the execution of sentences; or security measures. This exclusion

only applies to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

- ***Cabinet or an Executive Council:*** the processing of personal information by the Cabinet and its committees, or the Executive Council of a province.

- ***Judicial functions:*** the processing of personal information relating to the judicial functions of a court.

- ***Journalistic, literary or artistic purposes:*** the processing of personal information solely for the purposes of journalistic, literary or artistic expression, to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression. Furthermore, where a responsible party who processes personal information for exclusively journalistic purposes is subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code of ethics will apply to the exclusion of POPIA.

- ***Regulator exemption:*** in terms of section 37 of POPIA, the Information Regulator may, by notice in the Government Gazette, grant an exemption to a responsible party if the public interest in the processing outweighs any interference with the privacy rights of the data subject or it involves a clear benefit to the data subject or third party that outweighs any interference with the right to privacy.

THE LAWFUL PROCESSING OF PERSONAL INFORMATION

POPIA prescribes eight conditions for the lawful processing of personal information. Responsible parties must ensure that they process personal information in accordance with these conditions, which are as follows:

Condition	Requirements
Condition 1: *Accountability* **Detailed in section 8 of POPIA**	The responsible party must ensure the conditions for the lawful processing of personal information are complied with at the time of determining the purpose and means of the processing, and during the processing itself.
Condition 2: *Processing limitation* **Detailed in sections 9 to 12 of POPIA**	Personal information must be processed lawfully and in a reasonable manner, and only if it is adequate, relevant and not excessive given the purpose for which it is processed. This also requires that information may only be processed with the consent of the data subject, subject to exceptions.
Condition 3: *Purpose specification* **Detailed in sections 13 and 14 of POPIA**	Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the

	responsible party, and should not be retained for longer than is necessary to achieve that purpose.
Condition 4: *Further processing limitation* **Detailed in section 14 of POPIA.**	The further processing of personal information should be compatible with the purpose for which it was collected.
Condition 5: *Information quality* **Detailed in section 16 of POPIA.**	The responsible party must take steps to ensure the personal information is complete, accurate, not misleading and updated where necessary.
Condition 6: *Openness* **Detailed in section 16 of POPIA.**	The responsible party must take reasonably practicable steps to ensure the data subject is aware of, amongst other things, what personal information is being collected, the source of the information, the purpose for which it is being collected, and the name and address of the responsible party.
Condition 7: *Security safeguards* **Detailed in sections 19 to 22 of POPIA.**	The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures, having regard to generally accepted information security practices and procedures.
Condition 8: *Data subject participation:* **Detailed in sections 23 to 25 of POPIA.**	Data subjects must be given the right to enquire whether personal information is held about the data subject, and be provided with the record or a description of the information held. Data subjects may further request a responsible party to correct or delete personal information about them if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

Special Personal Information

POPIA prohibits the processing of special personal information, subject to the following exceptions:

- ***Consent:*** the processing is carried out with the consent of the data subject.
- ***Legal right or obligation:*** the processing is necessary for the establishment, exercise or defence of a right or obligation in law.
- ***International public law:*** the processing is necessary to comply with an obligation of international public law.

- ***Historical, statistical or research purposes:*** the processing is for historical, statistical or research purposes. This is further subject to the requirement that the purpose of the processing serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

- ***Deliberate publication:*** the information has deliberately been made public by the data subject.

The Information Regulator may authorise a responsible party to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject. Further, specific exclusions apply to each type of special personal information in sections 28 – 33 of POPIA. Not all of these are relevant for the purposes of this manual, however; we wish to note that the prohibition on processing personal information concerning a data subject's race or ethnic origin does not apply if the processing is carried out to identify data subjects, only when this is essential for that purpose, and to comply with laws and other measures designed to protect or advance persons disadvantaged by unfair discrimination.

Accordingly, it is important to understand whether you process personal information and if doing so is necessary, to establish the applicability of one of the above exclusions.

The Rights of Data Subjects

A data subject has the right to have his, her or its personal information processed lawfully. POPIA provides data subjects with certain rights, which include the following:

- ***Notification:*** the right to be notified that their personal information is being processed or accessed by an unauthorised person.

- ***Access:*** the right to establish whether a responsible party holds personal information about them and to request access to it.

- ***Correction, destruction or deletion:*** the right to request the correction, destruction, or deletion of their personal information.

- ***Objection:*** the right to object to the processing of their personal information.

- ***Direct marketing:*** the right not to have their personal information processed for direct marketing.

- ***Automated decision-making:*** the right not to be subject to a decision which is based solely on automated processing of their personal information.

- ***Redress:*** the right to submit a complaint to the Information Regulator regarding an interference with their personal information, or to institute civil proceedings regarding an interference with the protection of their personal information.

In the event that a data subject exercises one of these rights, your organisation must be able to respond appropriately and effectively. It is accordingly necessary that they be considered when implementing compliance measures.

The Responsibilities under POPIA

POPIA requires that the Responsible Party must ensure compliance with all of the lawful conditions for the processing of personal information. They remain responsible for the personal information, even when it is processed by an operator on behalf of the responsible party.

Further, POPIA requires that every Responsible Party designate an individual within their organisation to be the information officer; such individual has specific responsibilities under POPIA. The responsibilities of operators and information officers are dealt with in more detail below.

The Responsibilities of Operators

POPIA applies to operators that process personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party. This means that if you use the services of a person or company and such service entails the processing of personal information on your behalf, then the following requirements must be met:

- The operator or person processing personal information may only **process such information with the knowledge or authorisation** of the responsible party;

- The operator must **treat the personal information as confidential** and not disclose it unless required by law or in the course of performing their duties;

- **A written contract or mandate** between the responsible party and the operator must ensure that the operator **establishes and maintains appropriate security measures**;

- The operator must be **required to notify the responsible party** immediately where there are grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person.

The Responsibilities of the Information Officer

The Information Officer is the individual within a responsible party who is designated to encourage compliance with POPIA and assist data subjects and members of the public with POPIA related requests. Information Officers are, by virtue of their positions, appointed automatically in terms of POPIA.

The Information Regulator has released Draft Guidelines which note the designation of information officers. For private bodies, the designations are as follows:

- If your organisation is a **natural person**: the sole proprietor who carries on any trade, business or profession but only in such capacity, is the designated information officer.

- If your organisation is a **partnership**: any partner or any person duly authorised by the partnership si the designated information officer.

- If your organisation is a **juristic person**: the chief executive officer or the managing director or equivalent officer of the juristic person or any person duly authorised by that officer is the designated information officer.

In terms of POPIA, the duties and responsibilities of the information officer include the following:

- to ensure the body complies with POPIA;
- to deal with requests made to the body in terms of POPIA; and
- to cooperate with investigations relating to the body.

In terms of the Regulations, the Information Officer must further:

- **Develop a compliance framework** which must be implemented, monitored and maintained;

- **Complete a personal information impact assessment** to ensure the existence of adequate measures for compliance with the conditions for the lawful processing of personal information;

- **Compile a manual** to ensure compliance with section 51 of PAIA;

- **Develop and implement a system** to process requests for access to information;

- **Conduct internal awareness sessions** in order to educate employees regarding the legal framework regulating personal information.

Information officers must be registered with the Information Regulator before they may take up their responsibilities. Registration commences on 1 May 2021 and further guidance on the registration process will likely be published by the Information Regulator in due course. In terms of section 7.1 of the Draft Guidelines, private bodies are required to appoint at least one deputy information officer, but may any number.

DIRECT MARKETING

The processing of personal information of a data subject for the purpose of direct marketing is prohibited unless certain exceptions apply.

This prohibition includes direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or email.

Direct marketing means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
b) Requesting the data subject to make a donation of any kind for any reason.

An **automatic calling machine** means a machine that is able to do automated calls without human intervention.

The prohibition on the processing of personal information for direct marketing does not apply if one or more of the following exceptions apply:

- ***Consent:*** the data subject has given his, her or its consent to the processing.
  Further requirements for this exception include the following:
  - The Responsible Party may only approach a data subject once to request consent;
  - Consent may only be requested if the data subject has not previously withheld consent; and
  - Consent must be requested in the prescribed manner and form. A template for the request for consent for the purpose of direct market is provided in **Annexure B.**
- ***Existing customer:*** the data subject is an existing customer of the responsible party.
  Further requirements for this exception include the following:
  - The responsible party must have obtained the data subject's contact information through the sale of a product or service;
  - The purpose of the direct marketing must be for the responsible party's own similar products or services; and
  - The data subject must be given a reasonable opportunity to object to the use of their personal information. Such objection must be –
    - Provided free of charge and in a manner which is free of unnecessary formality; and
    - Provided to the data subject on the occasion of each communication with the data subject for the purpose of direct marketing.

Any communication for the purpose of direct marketing must contain the following:

- Details of the identity of the sender or the person on whose behalf the communication has been sent; and
- An address or other contact details to which the recipient may send a request for such communication to cease.

AUTOMATED DECISION- MAKING

POPIA provides that a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person. This includes performance at work, creditworthiness, reliability, location, health, personal preferences or conduct.

Automated decision-making is not defined in POPIA.

The UK ICO explains it as:

"the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiled or inferred data."

Profiling is also not defined in POPIA.

The UK GDPR defines profiling in article 4(4) as:

"any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

The UK ICO explains that:

"Organisations obtain personal information about individuals from a variety of different sources. Internet searches, buying habits, lifestyle and behaviour data gathered from mobile phones, social networks, video surveillance systems and the Internet of Things are examples of the types of data organisations might collect.

They analyse this information to classify people into different groups or sectors. This analysis identifies correlations between different behaviours and characteristics to create profiles for individuals. This profile will be new personal data about that individual."

The prohibition on automated decision-making does not apply if one or more of the following exceptions is applicable:

- ***Contractual provision:*** the decision has been taken in connection with the conclusion or execution of a contract. Furthermore, the request of the data subject in terms of the contract must be met; or appropriate measures must have been taken to protect the data subject's legitimate interests.

- ***Law or code of conduct:*** the decision is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

The reference to **appropriate measures** requires that the data subject must be provided with an opportunity to make representations about the decision; and the responsible party must provide the data subject with sufficient information about the underlying logic of the automated processing of information to enable him or her to make such representations.

CROSS-BORDER DATA TRANSFERS

The transfer of personal information about a data subject to a third party who is in a foreign country is prohibited, unless one or more of the following exceptions apply:

- ***Adequate level of protection:*** the third party who is the recipient of the information is subject to a law, binding corporate rules or a binding agreement which provide an adequate level of protection which:
    - upholds the principles for reasonable processing of the information that are substantially similar to the conditions for lawful processing included in POPIA;
    - includes provisions relating to the onward transfer to subsequent third parties in foreign countries which are substantially similar to POPIA's provision on cross-order data transfers.

> **Binding corporate rules** are defined to mean:
>
> Personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertaking in a foreign country.
>
> A **group of undertakings** means a controlling undertaking and its controlled undertakings.

- ***Consent:*** the data subject consents to the transfer.
- ***Performance of a contract:*** 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 taken in response to the data subject's request.
- ***Conclusion or performance of a contract:*** 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.
- ***Benefit of the data subject:*** the transfer is for the benefit of the data subject; it is not reasonably practicable to obtain the consent of the data subject to that transfer; and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

POPIA requires that responsible parties must obtain **prior authorisation from the Information Regulator** if that responsible party plans to transfer special personal information or personal

information concerning a child to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

ROLE OF THE INFORMATION REGULATOR

POPIA establishes the Office of the Information Regulator, which is empowered to monitor and enforce compliance by public and private bodies with POPIA and PAIA. The Information Regulator is an independent juristic entity which is accountable to the National Assembly of Parliament.

The Powers, Functions and Duties of the Information Regulator

The Information Regulator is mandated to provide education, handle complaints and conduct research.

Importantly, the Information Regulator is empowered to investigate allegations of violations of the provisions of POPIA which it may do so following a complaint or on its own initiative. If there are reasonable grounds to suspect that a responsible party is interfering with the protection of personal information or that an offence under POPIA has been committed, the Information Regulator may apply for a warrant. The warrant may empower the Information Regulator to enter and search premises and inspect, examine, operate, or test any equipment which is used for the processing of personal information. It further allows the Information Regulator to seize any record, material or equipment as evidence.

If a responsible party is found to be interfering with the protection of personal information, the Information Regulator may serve them with an enforcement notice. Such a notice may either specify steps which must be complied with or specify the prohibition of processing. Non-compliance with such a notice is an offence.

Prior Authorisation

Prior authorisation from the Information Regulator is required if a responsible party intends to process information in the following ways:

- ***Unique Identifiers:*** the responsible party wishes to process any unique identifiers of data subjects for a purpose other than the one specifically intended at collection with the intention of linking the information with information processed by other responsible parties;

  > A **unique identifier** is any identifier assigned to a data subject which is used by a responsible party for the purpose of their operations and that uniquely identifies that data subject in relation to that responsible party. For example, a National Identity Number.

- ***Criminal Behaviour:*** the responsible party wishes to process information concerning criminal behaviour or unlawful or objectional conduct on behalf of third parties;

- ***Credit Report:*** the responsible party wishes to process information for the purpose of credit reporting;

- ***Cross-border transfer:*** the responsible party wishes to transfer special personal information or the information concerning children to a third party in a foreign country that does not provide an adequate level of protection.

Prior authorisation is only required once – not each time the information is processed, but it must be obtained again if the processing departs from what was originally authorised. Prior authorisation is **not required** if regulated in a code of conduct which is in force and binding on a specific sector.

The Regulator may require prior authorisation for additional types of processing which carry a particular risk for the legitimate interests of the data subject. Notice of theses additions will be published by law or regulation.

Processing in the above ways cannot begin until the Information Regulator has authorised it. The Information Regulator will conduct an investigation and may authorise the processing or notify the responsible party that a more detailed investigation is required. A detailed investigation may take up to 13 weeks to complete and the Information Regulator will provide a statement on the lawfulness of the processing.

CONSEQUENCES OF NON-COMPLIANCE

POPIA creates certain criminal and civil offences for non-compliance with the Act which may result in **imprisonment of up to 10 years** or a **fine of up to R 10 million.**

When determining an appropriate fine, some of the factors considered by the Information Regulator include: the nature of the personal information involved; the duration and extent of the contravention; the number of data subjects affected by the contravention; whether the responsible party or third party could have prevented the contravention; any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information; and any previous offences committed under POPIA.

Importantly, POPIA provides for the institution of civil proceedings for non-compliance with POPIA. A data subject, or the Information Regulator acting on their behalf, may institute an action for damages against a responsible party regardless of whether non-compliance was negligent or intentional.

Beyond these sanctions non-compliance carries the possibility of reputational harm which can far-reaching consequences for organisations.

PRACTICAL STEPS FOR IMPLEMENTATION

In implementing compliance measures, we encourage organisations to find a tailored approach which gives meaningful effect to the constitutional rights to privacy and access to information, is

legally compliant, and enables the processing of personal information.

Although the measures required to ensure compliance with POPIA may differ depending on the size and operation of an organisation, we have provided several general steps for implementation which may help guide or inform your implementation process.

Implementation Step	Things to Consider
Preliminary Measures	
Determine if POPIA applies	Remember to assess whether one of the exclusions apply.
Appoint an Information Officer	If your organisation is a private body, section 5 of the Draft Guidelines requires that the Information Officer must be the Chief Executive Officer or the Managing Director or equivalent officer.
Register the Information Officer with the Information Regulator	Registration with the Information Regulator commences on 1 May 2021. The process for registration will likely be published by the Information Regulator in due course.
Appoint a Deputy Information Officer	Section 7(2) of the Draft Guidelines requires that public and private bodies appoint a deputy information officer. More than one deputy information officer may be designated depending on the size, structure and complexity of the operations of a specific body.
Conduct a gap analysis in order to review your organisation's operations to determine current levels of compliance	Such an analysis should outline the ways in which your organisation is currently processing personal information, as well as special personal information. It should include an action plan which details the next steps which are necessary to implement compliance. Such an analysis may include a data inventory which could assist in understanding all the different types of personal information processed by your organisation. A data inventory template is provided in **Annexure C.**
Ensuring Compliance with the Eight Conditions for Lawful Processing	

Requirements of Condition 1: Accountability • **The responsible party must ensure compliance with the provisions of POPIA;** • **The responsible party is responsible throughout the lifecycle of processing activities;** • **The responsible party cannot contract out of this responsibility – the responsible party must ensure that reasonable measures are put in place to ensure that third-party operators comply with the provisions of POPIA.**	
Review all internal policies.	If necessary, amend or develop a comprehensive data protection policy to guide the internal processing and management of personal information. Attention must be paid to the processing of personal information on an organisation's website and if necessary, a cookie policy and terms of use must be amended or developed.
Develop a personal information impact assessment.	Regulation 4(1) of the Regulations requires that the Information Officer conducts a personal information impact assessment to ensure that adequate measures and standards exist to comply with the lawful processing of personal information.
Requirements of Condition 2: Processing Limitation • **Ensure that the processing of personal information is lawful and observant of the data subject's right to privacy.** • **Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.** • **Establish one or more justifications for the personal information that is processed.** • **If consent is the ground of justification relied upon, such consent must be a voluntary, specific and informed expression of will.** • **A data subject may object, at any time, to the processing of personal information, on reasonable grounds relating to his, her or its personal situation, unless legislation provides for such processing.** • **As a general position, personal information must be collected directly from the data subject, subject to certain exceptions.**	
Undertake an internal review to determine whether the amount of personal information you collect is necessary to achieve the purpose.	Ensure that you are not collecting an excessive amount of personal information.
Review the processes through which consent is requested.	If necessary, develop a consent form which includes sufficient information concerning the purpose for the collection in order to ensure

	that consent is specific and informed.
Develop an internal process or system to capture and store consent.	In terms of section 11(2)(a) of POPIA, a responsible party bears the burden of proof that the consent relied upon has been appropriately obtained.
A formal process must be implemented to record, address, capture and effect objections and withdrawals of consent for the processing of personal information.	
Requirements of Condition 3: Purpose Specification • **Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.** • **Take steps to ensure that the data subject is made aware of the purpose of the collection of the personal information.** • **As a general position, records of personal information must not be retained for any longer than is necessary to achieve the purpose for which the information was collected or subsequently processed, subject to exceptions.** • **Records of personal information may be retained for longer periods for historical, statistical or research purposes, provided that the responsible party has established appropriate safeguards against the records being used for any other purposes.** • **If a record of personal information is used to make a decision about a data subject, the responsible party is required to retain the record for the period prescribed by law, or if no such law exists, for a period that will afford the data subject a reasonable opportunity to request access to the record.** • **Destroy, delete or de-identify a record of personal information as soon as reasonably practicable after it is no longer authorised to retain the record.** • **Restrict the processing of personal information, if its accuracy is contested by a data subject, for a period to enable verification of the accuracy of the information.**	
Develop and implement a process which ensures that the data subject is aware of the purpose for collection of information at each collection point.	
Develop a records retention schedule for the different categories of personal information that are collected and retained.	
Requirements of Condition 4: Further Processing Limitation • **Further processing of personal information must be in accordance or compatible with the purpose for which the information was collected.** • **The further processing of personal information is not incompatible with the purpose of collection if the information is used for historical, statistical or research purposes, and the responsible party ensures that it is carried out solely for such purposes and will not be published in an identifiable form.**	

<table>
<tr><td colspan="2">• The responsible party may seek consent from the data subject for the further processing of personal information.</td></tr>
<tr><td>Define and implement a formal process to determine whether further processing is compatible with the original purpose of collection.</td><td></td></tr>
<tr><td colspan="2">Requirements of Condition 5: Information Quality

• Reasonably practicable steps must be taken to ensure that personal information is complete, accurate, not misleading and updated where necessary.</td></tr>
<tr><td>Undertake a data cleansing exercise for existing data.</td><td>Consider sending a notification to all data subjects indicating that their personal information requires review.</td></tr>
<tr><td>Provide facilities for data subjects to update their personal information.</td><td></td></tr>
<tr><td colspan="2">Requirements of Condition 6: Openness

• The responsible party is required to maintain the documentation of all processing operations under its responsibility.
• Where personal information is collected, the responsible party is required to take reasonably practicable steps to ensure that the data subject is aware of all relevant information, including the information being collected; the name and address of the responsible party; the purpose for which the information is being collected; the consequences of failure to provide the information; and whether it intends to transfer the personal information to a third party outside of South Africa.</td></tr>
<tr><td>Review all hard-copy and electronic forms that are used to collect personal information to ensure that the required information is provided to data subjects at the point of collection.</td><td>If necessary, update or develop such forms to ensure compliance with POPIA.</td></tr>
<tr><td colspan="2">Requirements of Condition 7: Security Safeguards

• The responsible party is required to secure the integrity and confidentiality of personal information in its possession or under its control, by taking appropriate, reasonable, technical and organisational measures to prevent any loss, damage, unauthorised destruction or unlawful access to personal information.
• This requires the responsible party to take reasonable measures to identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; establish and maintain appropriate safeguards against</td></tr>
</table>

the risks identified; regularly verify that the safeguards are effectively implemented; and ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. • An operator or anyone processing personal information on behalf of a responsible party or an operator, must process such information only with the knowledge or authorisation of the responsible party; and treat personal information which comes to their knowledge as confidential. • The responsible party is required to establish written contracts with all operators to ensure that the operator maintains appropriate security safeguards, and to expressly require the operator to notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person. • In the event that there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the responsible party will be required to notify the Information Regulator and the affected data subjects.	
Review existing internal security measures.	If necessary, amend or improve information security measures to ensure compliance with POPIA.
Conduct regular information security risk assessments.	Such assessments should aim to identify all reasonably foreseeable internal and external risks to personal information.
Review all existing contracts with third-party operators who process information on your behalf.	If necessary, the agreements must be amended or developed to ensure that that the operator establishes and maintains appropriate security safeguards, and to expressly require the operator to notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person.
Establish a robust privacy response programme, that is well-publicised and generally known within the organisation. **This should cover privacy and data security breaches for both electronic and hard-copy records, and allow the centralised and expeditious reporting of any such breaches.**	POPIA does not prescribe a specific timeframe within which notification of a breach must be provided to the information regulator or the data subject. Such notification must be provided as soon as reasonably possible.
Requirements of Condition 8: Data Subject Participation	

• The data subject, having provided adequate proof of identity, has the right to request the responsible party to confirm, free of charge, whether it holds personal information about the data subject. • The data subject has the right, having provided adequate proof of identity, to request the responsible party to provide the record or description of the personal information about the data subject held by it, including information about all third parties who have had access to the information, within a reasonable time, at a prescribed fee (if any), in a reasonable manner and format, and in a form that is generally understandable. • A data subject is entitled to request the correction or deletion of their personal information if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully. A data subject may also request the destruction or deletion of a record of personal information if the responsible party is no longer authorised to retain that record. • In the event that the responsible party receives a request as set out above, it must as soon as reasonably practicable, correct the information; destroy or delete the information; provide the data subject with credible evidence in support of the information; or, where agreement cannot be reached, and if the data subject so requests, take reasonable steps to attach the request for correction to the record.	
Implement a formal process to execute and manage requests from data subjects.	Such a process should include how to identify a data subject; acceptable formats for requests and how to respond to a request made other than in such format; where to refer such requests; authentication procedures; how to log requests; what information needs to be disclosed; any exceptions to disclosure and the reasons for such exceptions; and notification to the data subject.
Additional Measures	
Conduct internal training.	Compliance with POPIA requires behavioural change and it is accordingly necessary that individuals within your organisation are aware of the requirements of POPIA and any operational changes.

KEY ISSUES FOR CONSIDERATION

Consent

Consent is one of the justifications for the lawful processing of personal information. If the data subject is a child, consent must be provided by a competent person.

Consent is defined in POPIA to mean any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

A data subject may withdraw consent at any time, provided that the withdrawal will not affect the lawfulness of the processing which occurred before the withdrawal of consent.

Cookies

Cookies are files with small pieces of data, such as a username, which are used to identify a specific computer. They "track, personalise and save information about each user's session" on a website.[20] Cookies' store information about the user's behaviour on the website and are often used to improve the ways in which the user interacts with the website. Cookies can sometimes collect and store personal information and must therefore be processed in compliance with POPIA. It is important to obtain the user's consent for the use of cookies.

GDPR and the Californian Consumer Privacy Act

The General Data Protection Regulation (GDPR) 2016/679 is the law which governs data protection and privacy in the European Union. Importantly, the law applies to the processing of personal information of European Union data subjects regardless of jurisdiction. This means that if a South African organisation collects and processes the personal information relating to a European Union data subject, it must process it in compliance with GDPR.

The California Consumer Privacy Act (CCPA) is a data protection law which was passed by California in 2018. The law came into effect on 1 January 2020 and was enforced from 1 July 2020.

The law applies to companies all over the world if their annual revenue is over $25 million, if they have the personal data of at least 50 000 people or more than half of their revenue comes from the sale of personal data. It is important to note that the CCPA has a broad definition of personal data which includes: email addresses, online handles, IP addresses and browsing and search history. In the event that the CCPA applies, processing personal data which falls within the ambit of the CCPA requires compliance.

CONCLUDING REMARKS

The right to privacy is a fundamental human right — one which enables the exercise of other important rights. The right is given effect through POPIA and accordingly compliance with the legislation enables the protection and promotion of the right.

We hope this manual assists you in finding an approach that gives meaningful effect to constitutional rights, is legally compliant and enables the processing of personal information as needed for your organisation.

[20] Kaspersky, 'What are cookies', available at https://www.kaspersky.com/resource-center/definitions/cookies.

ANNEXURE A: GLOSSARY OF TERMS

Data message	**Data generated, sent, received or stored by electronic means, including –** • **voice, where the voice is used in an automated transaction; and** • **a stored record.**
Data subject	The person to whom personal information relates.
Direct marketing	To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of – • promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or • requesting the data subject to make a donation of any kind for any reason.
Electronic communication	Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
Operator	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
Personal information	Information relating to an identifiable, living, nature person, and where it is applicable, an identifiable, existing juristic person, including but not limited to – • information relating to the 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; • information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; • the biometric information of the person; • the personal opinions, views or preferences of the person; • correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further

	correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about the person; and • the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
Processing	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including – • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as restriction, degradation, erasure or destruction of information.
Record	Regardless of the form or medium, including any of the following: • writing on any material; • information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; • label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means; • book, map, plan, graph or drawing; • photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; in the possession or under the control of the responsible party, whether or not it was created by the responsible party, and regardless of when it came into existence.
Responsible party	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
Special personal	The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life,

information	or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
Unique identifier	Any identifier that is assigned to a data subject and used by a responsible party for the purposes of the operations of that responsible party, and that uniquely identifies that data subject in relation to that responsible party.

ANNEXURE B: CONSENT CLAUSE FOR DIRECT MARKETING

Application for the consent of a data subject for the processing of personal information for direct marketing in terms of section 69(2) of POPIA	
Part A	
To:	_____ [Insert name of data subject]
From:	_____ [Insert name of responsible party]
Contact details:	_____ _____ [Insert address and contact details – including contact number, fax number and email address] – of responsible party]
Full names and designation:	_____ _____ [Insert full names and designation of person signing on behalf of the responsible party]
Signed at _____ on this ____ day of _____ 20____. Signature of designated person: _____	
Part B	
I, _____ (full names of data subject), hereby: ☐ Give my consent to receive direct marketing of goods or services to be marketed by means of electronic communication.	
Goods or services:	_____ [Specify goods or services]
Method of communication:	☐ Fax: ☐ Email: ☐ Others (specify):
Signed at _____ on this ____ day of _____ 20____. Signature of data subject: _____	

ANNEXURE C: DATA INVENTORY

Identification[21]	When collected[22]	What collected[23]	Justification and purpose[24]	Data storage[25]	Third party access[26]	Transborder transfers[27]	Correction or deletion[28]	Verification of accuracy[29]	Deletion or destruction[30]

[21] **Identification:** This refers to the identification of the data subject. This should also capture the category of the data subject (e.g. whether the data subject is a client, the subject of a research report, an employee, etc).
[22] **When collected:** This refers to the date on which the Personal Information was collected.
[23] **What collected:** This refers to the categories of Personal Information collected. This should not reflect the specific details of the Personal Information, but rather the broad categories of Personal Information (e.g. name, identity number, contact details, etc).
[24] **Justification and purpose:** This should reflect whether consent has been obtained, or whether there is another ground of justification being relied upon. Further, the purpose(s) for the processing of Personal Information should be captured (e.g. for litigation, research, employment, etc).
[25] **Data storage:** This refers to whether the Personal Information is being stored electronically or in hard-copy.
[26] **Third-party access:** This should reflect any third parties with whom the Personal Information is shared, as well as any measures that have been put in place to safeguard the protection of the Personal Information (e.g. a third party for the purpose of storage, subject to a written contract).
[27] **Transborder transfers:** This should reflect any third parties based in a foreign country with whom the Personal Information is shared, the country in which the third party is based, and the purpose for the sharing of the Personal Information.
[28] **Correction or deletion:** This refers to whether there have been any requests from the data subject for the correction or deletion of their Personal Information, and the response to that request.
[29] **Verification of accuracy:** This refers to whether any steps have been taken to verify the accuracy of the Personal Information following the initial collection thereof.
[30] **Deletion or destruction:** This should reflect whether the Personal Information has been deleted, destroyed or de-identified. It may also be used to record when Personal Information will need to be deleted or destroyed.

ANNEXURE D: LIST OF SUGGESTED RESOURCES

Legal Frameworks

South Africa

- Promotion of Access to Information Act 2 of 2000: https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf
- Protection of Personal Information Act 4 of 2013: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf
- Regulations Relating to the Protection of Personal Information, 2018: https://www.justice.gov.za/inforeg/docs/20181214-gg42110-rg10897-gon1383-POPIregister.pdf
- Draft Guidelines on The Registration of Information Officers, 2020: https://www.justice.gov.za/inforeg/docs/InfoRegSA-Guidelines-InfoOfficers-Invite-20200717.pdf

Europe

- General Data Protection Regulation 2016/679: https://gdpr-info.eu/

United Kingdom

- Data Protection Act, 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

United States

- California Consumer Privacy Act, 2018: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=
- California Consumer Privacy Act Regulations, 2020: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf?

Resource guides

- ALT Advisory, 'Is POPIA compliance sufficient to meet the requirements of the GDPR?', 2018: https://altadvisory.africa/2018/04/25/is-popia-compliance-sufficient-to-meet-the-requirements-of-the-gdpr/

- IAB Europe, 'TCF – Transparency and Consent Framework', 2019: https://iabeurope.eu/transparency-consent-framework/

- ICO, 'Direct marketing', 2018: https://ico.org.uk/media/1555/direct-marketing-guidance.pdf

- Access to information request form A – for use when information is held by a public body: https://www.justice.gov.za/forms/paia/J750_paia_Form%20A.pdf

- Access to information request form C – for use when information is held by a private body: https://www.justice.gov.za/forms/paia/J752_paia_Form%20C.pdf

iab south africa

Visit iabsa.net