Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 696 30 June Junie 2023 No. 48865

PART 1 OF 3

ISSN 1682-5845

9 771682 584003 48865

DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

NO. 3627 **30 June 2023**

INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Address: 27 Stiemens Street, 4th Floor
JD House Building, Braamfontein,
Johannesburg, 2017
Tel: 010 023 5214
Fax: 0865003351
E-mail: POPIACompliance@inforegulator.gov.za

14 June 2023

NOTICE IN TERMS OF SECTION 61(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA) CODE OF CONDUCT: THE DIRECT MARKETING ASSOCIATION OF SOUTHERN AFRICA (DMASA).

1. In terms of the provisions of section 61(2) of POPIA, the Information Regulator (Regulator) gives notice that the Regulator is in receipt of a proposed code of conduct from the Direct Marketing Association of Southern Africa (DMASA) that deals with how personal information will be processed in the Direct Marketing Industry.

2. The purpose of the code of conduct is to-
   2.1. promote appropriate practices by members of DMASA governing the processing of personal information in terms of POPIA;

   2.2. encourage the establishment of appropriate agreements between members of DMASA and third parties, regulating the processing of personal information as required by POPIA and dictated by good business practice; and

   2.3. to establish procedures for members of DMASA to be guided in their interpretation of principally POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against DMASA to be considered and remedial action, where appropriate, to be taken.

3. The code of conduct governs-
   3.1. the processing of personal information (including personal information of data subjects) by institutions that are members of DMASA.

3.2. where appropriate, agreements that may need to be concluded between members of DMASA and third parties promoting, and to the extent possible ensuring that personal information is processed in compliance with POPIA; and

3.3. the enforcement by DMASA of the provisions of the code of conduct.

4. A notice will be published in the Government Gazette in compliance with section 61(2) of POPIA. Affected persons are invited to submit written comments to the Regulator email address: POPIACompliance@inforegulator.org.za. within fourteen (14) days after publication of the notice in the Government Gazette. A copy of the proposed code of conduct will be made available on the Regulator's website, alternatively, a request for a copy of the code may be made by addressing correspondence to email address:
POPIACompliance@inforegulator.org.za

Direct Marketing POPIA

Code of Conduct

[E] info@dmasa.org [W] www.dmasa.org [A] Fernridge Office Park, 5 Hunter Street, Ferndale
Direct Marketing Association of South Africa Reg. No.: 2005/040417/08 | VAT No.: 4650231352

Contents

Direct Marketing POPIA 0
Code of Conduct 0
1. About the Direct Marketing Association of South Africa 2
2. About this POPIA Code of Conduct 2
3. The scope of the Code 3
4. Consider whether other legislation applies 4
5. Determine who must ensure that direct marketing activities comply with this Code 4
6. Perform a personal information impact assessment 9
7. Authorisations 27
8. Enforcement of the Code 28
9. Independent adjudicator 33
10. Administration of the Code 33
11. Review and expiry of the Code 34
12. Glossary 34

1. About the Direct Marketing Association of South Africa

The Direct Marketing Association of South Africa (DMASA) is an independent body that companies in the Direct Marketing industry set up and pay for to ensure that the industry's self-regulation system works in the public's interest. DMASA is a voluntary membership association.

DMASA has developed this POPIA Code of Conduct (Code) to ensure that all DMASA members comply with the requirements of POPIA when they engage in Direct Marketing Activities. Once this POPIA Code of Conduct is recognised under POPIA, this POPIA Code of Conduct shall be enforceable against all DMASA members. DMASA has engaged other industry associations and direct marketers in drafting this Code to ensure that these stakeholders were consulted, and their feedback is taken into account.

2. About this POPIA Code of Conduct

2.1. The purpose of this Code

The purpose of this Code is to:

- make it clear to DMASA members how to comply with POPIA when engaging in Direct Marketing and mitigate POPIA compliance risk;
- express DMASA's interpretation of POPIA;
- raise the standards of good conduct in the Direct Marketing industry without endangering the vitality and growth of business;
- create a panel of experts to adjudicate complaints related to Direct Marketing;
- provide a consistent, accessible and efficient system for the consensual resolution of disputes arising from the Processing of Personal Information;
- provide safeguards when Responsible Parties link datasets for Direct Marketing purposes; and
- Educate Data Subjects as to their rights and redress available to them, should a DMASA member breach POPIA or this Code.

2.2. Commencement of the Code

This Code will come into effect 28 days after the Regulator issued the Code and published a notice in the Government Gazette.

DMASA will publish the commencement date of the Code on its website with a copy of the issued Code.

2.3. Defined terms and footnotes

If a word is capitalised, it is defined in the Glossary.

Footnotes have been included to document the rationale behind specific provisions and facilitate a review of the Code. Once the Regulator issues the Code, these footnotes will be removed.

3. The scope of the Code

This Code applies to DMASA members when they engage in Direct Marketing Activities. The Code will apply to any Direct Marketing Activity where Personal Information is Processed after the effective date of the Code, regardless of when the Direct Marketing Activity started. The Code does not apply retrospectively.

For instance, a Responsible Party collected Personal Information in 2018 and used that Personal Information for Direct Marketing after the Code became effective. The Code does not apply to the collection of Personal Information, but the Direct Marketing Activities engaged after the effective date of the Code must comply with the Code.

Direct Marketing Activities include all the activities in a Direct Marketing[1] process that involve Processing Personal Information. For instance:

- collecting Personal Information for Direct Marketing
- lead generation for Direct Marketing
- profiling Data Subjects for purposes of Direct Marketing
- sending Direct Marketing messages
- telemarketing
- managing Data Subjects' Direct Marketing consent
- asking Data Subjects for donations
- destroying or deleting Personal Information used for Direct Marketing

If you answer 'yes' to all of the following questions, then this Code applies:

- **Are you Processing identifiable Personal Information?** Processing includes collecting, creating, sharing, transforming, storing, or destroying Personal Information.[2] Identifiable Personal Information is any information related to a living individual or an existing juristic person (e.g., a company or other organisation) that can make it possible to identify that individual or juristic person.[3] The Code does not apply to indirepermanently De-identified information.[4]

---

[1] Section 1 of POPIA defines 'Direct Marketing' as meaning '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.'

[2] See the definition of Processing, section 1 of POPIA and the Glossary.

[3] See the definition of Personal Information, section 1 of POPIA and the Glossary.

[4] Section 6(1)(b) of POPIA.

- **Is the purpose of Processing Personal Information related to Direct Marketing?** Direct Marketing is the Processing of Personal Information to approach a Data Subject to promote or offer to supply goods or services to the Data Subject or ask the Data Subject for a donation.[5]
- **Is the Processing taking place in South Africa?** The Code applies to all Responsible Parties based in South Africa who engage in Direct Marketing Activities in South Africa.[6]

4. Consider whether other legislation applies

DMASA members' Direct Marketing Activities may be governed by other legislation, regulations, or codes of conduct. If other binding legislation, regulations, or codes of conduct provide more extensive protection of Personal Information or the rights of Data Subjects, the member must comply with the most extensive requirements.

5. Determine who must ensure that direct marketing activities comply with this Code

5.1. The roles and responsibilities in direct marketing activities

POPIA introduced the concept of a Responsible Party. The Responsible Party is the public or private body or a person who, alone or with others, determines why and how Personal Information is Processed.[7]

The Regulator and Data Subjects will hold the Responsible Party liable if they do not comply with POPIA.[8] The Responsible Party must ensure that Direct Marketing Activities comply with POPIA before the activities begin and until they are completed.[9]

When an organisation generates its own leads and manages its own Direct Marketing, it is accountable in terms of POPIA and must comply with POPIA, but when it relies on others to generate leads or to market on its behalf, their roles in the Direct Marketing Activity will

---

[5] See the definition of Direct Marketing, section 1 of POPIA.

[6] Section 3(1)(b) states that '(POPIA) applies to the processing of personal information where the responsible party is domiciled in the Republic; or 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'. Organisations are domiciled in South Africa if they meet the definition of 'resident' in section 1 of the Income Tax Act 58 of 1962. This will be the case if the organisation is incorporated, established or formed in South Africa, or if it has its 'central management and control' in South Africa.

[7] See the definition of Responsible Party, section 1 of POPIA.

[8] Section 8 states that the Responsible Party must ensure that the conditions for lawful Processing of Personal Information are met. Except for sections 20 and 21, the conditions all refer to the 'responsible party'.

[9] See condition 1: accountability, section 8 of POPIA.

determine who is accountable. They may be independent Responsible Parties, co-Responsible Parties, or Operators:

Role	Legal implication
Independent Responsible Parties	Responsible Parties are organisations or individuals who determine the **purpose** of and **means** for Processing Personal Information. Responsible Parties decide: • why ('to what end' or 'what for') Personal Information is Processed • how (which means to employ to reach the objective) Personal Information is Processed • what Personal Information to Process • how long to Process Personal Information • who has access to the Personal Information • which Operators to appoint to Process Personal Information on their behalf Responsible Parties are accountable for complying with the Code.
Co-Responsible Parties	Co-Responsible Parties work towards a common purpose and make joint decisions when Processing Personal Information.[10] Each Co-Responsible Party is necessary for the Processing to take place and has a tangible impact on determining the purpose and means of Processing. More than one Responsible Party may be co-Responsible Parties for certain parts of a Direct Marketing Activity and independent Responsible Parties for the other parts of the Direct Marketing Activity. Co-Responsible Parties are jointly responsible when they process Personal Information; this means that the Regulator and Data Subjects can choose who to hold liable should any of the Co-Responsible Parties not comply with the Code.

[10] The definition of Responsible Party in section 1 of POPIA explicitly allows for multiple responsible parties that act together.

	They can also choose to hold co-Responsible Parties liable together.[11]
Operators	An Operator is a person or organisation that processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party.[12] So, employees (as defined by labour law) are not Operators. Operators may make decisions about non-essential aspects of a Processing activity. The Regulator and Data Subjects will hold the Responsible Party liable if an Operator does not comply with the Code. The Responsible Party can hold the Operator liable in terms of a contract. If a Responsible Party (or parties) uses an Operator, they must agree in writing that the Operator will comply with the Code's security safeguards.

5.2. Identify the responsible party, co-responsible parties, and operators

DMASA members who undertake Direct Marketing Activities with others must conduct an accountability assessment to:

- identify the Responsible Party, co-Responsible Parties and Operator(s); and
- conclude the appropriate agreements.

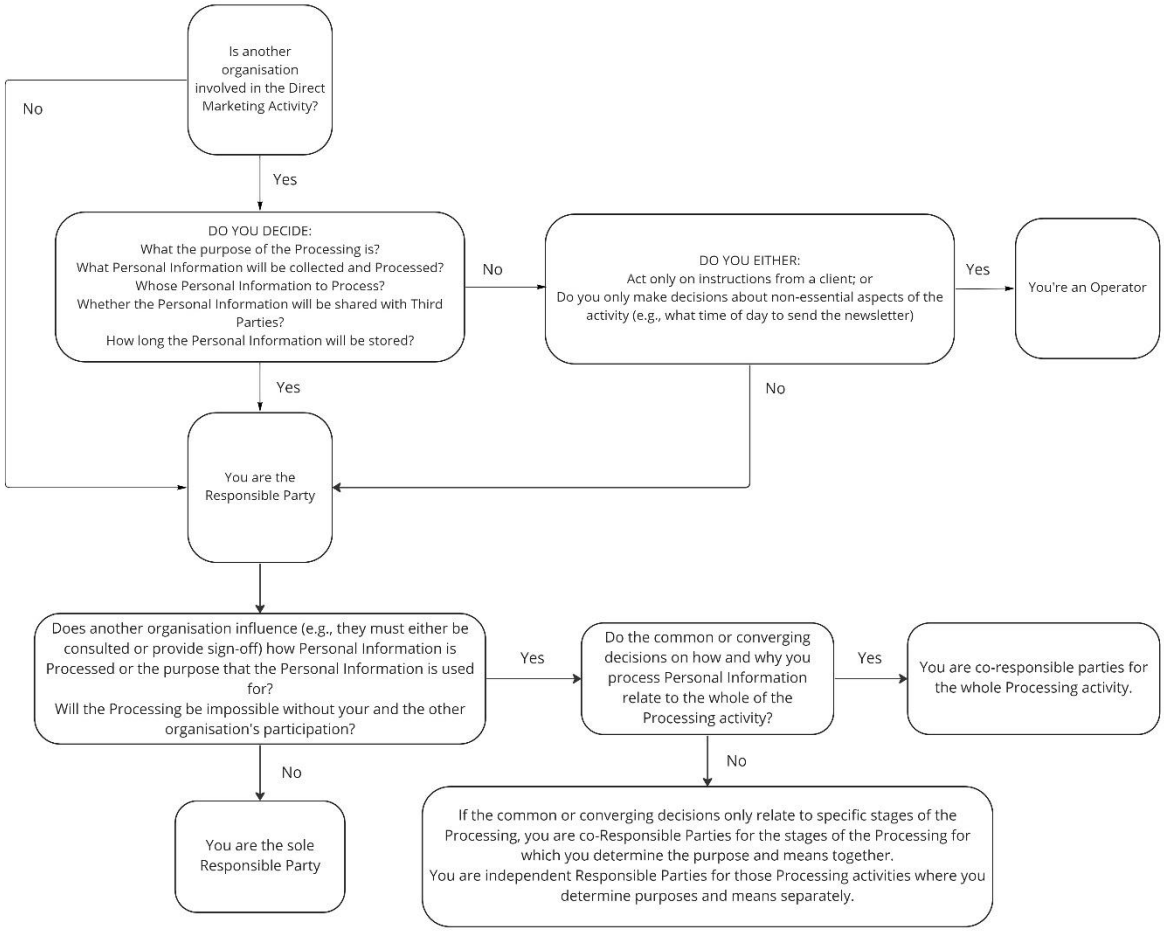
DMASA members can use the flowcharts and tables below to distinguish between Responsible Parties, co-Responsible Parties and Operators. When DMASA members perform an accountability assessment, members must also take the following factors into account:

- the factual circumstances related to the Processing activities;
- any agreements underpinning the relationships between the parties;

[11] POPIA is not clear on how liability will be apportioned. Commentary under the EU Data Protection Directive states that unless the co-responsible parties or the factual circumstances indicate otherwise, the liability will be joint and several. Please *see Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor'* 24, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[12] See the definition of Operator, section 1 of POPIA.

- the Data Subject's understanding of the Processing activities and the responsibilities of the parties involved.



Factors that indicate you are a Responsible Party	Factors that indicate you are an Operator
You obtain benefit from or have an interest in, the Processing.	You Process the Personal Information for another organisation's purposes and according to its documented instructions.
You make decisions about Data Subjects as part of or because of the Processing.	Another organisation monitors your Processing activities to ensure that you comply with instructions and terms of a contract.

The Processing activities are naturally attached to your role (e.g., a retailer Processing their customers' Personal Information to receive account payments).	You do not pursue your own purpose in the Processing other than your own business interest to provide services.
The Processing refers to your relationship with the Data Subjects as employees, members, customers etc.	You have been engaged to carry out specific Processing activities by someone who, in turn, has been engaged to Process Personal Information on another organisation's behalf and that organisation's documented instructions. In this case, you are a sub-Operator.
You have complete autonomy in deciding how Personal Information is Processed.	
You have authorised an external organisation to Process Personal Information on your behalf.	

5.3. Accountability checklist for responsible parties

All Responsible Parties must:

- ☐ **Appoint an Information Officer** and Deputy Information Officer(s) where the size of the Responsible Party justifies it, who must ensure compliance with the Code. Information Officers and Deputy Information Officer(s) must be registered with the Regulator.[13] The Information Officer and Deputy Information Officer(s) 's roles must be described in writing and explicitly refer to the Code.
- ☐ Create a **POPIA compliance framework**.[14] This framework must document how the Responsible Party will implement the Code in their policies, procedures, standards, templates, and other binding documents. These documents must set out the responsibilities for different Direct Marketing-related roles. At least once every two years, the Information Officer and Deputy Information Officer(s) must review and audit that these documents comply with POPIA.

[13] See the Information Regulator's Guidance Note on Information Officers and Deputy Information Officers for further guidance.

[14] POPIA regulation 4(a).

- Create, publish, and implement a **Promotion of Access to Information Act** (PAIA) **manual**.[15]
- Complete and document a **Personal Information Impact Assessment** (PIIA) before new Direct Marketing Activities start.[16] When a Direct Marketing Activity is the same or similar to a previous activity that was assessed previously, the Responsible Party may rely on the previous assessment.
- Ensure that everyone involved in Direct Marketing Activities receives **training** on their data protection responsibilities.[17]

If more than one organisation participates in the Direct Marketing Activity, the Responsible Party must also:

- identify the Responsible Party(s), co-Responsible Parties, and Operators involved in the activity;
- conclude agreements with Operators in which they agree:
    - to limit the use of Personal Information to instances where it has the Responsible Party's written authority,
    - that the Personal Information is confidential and that they must not share it with Third Parties without the Responsible Party's written authority,
    - to implement appropriate security safeguards (equivalent to or stricter than the security safeguards section of this Code) when Processing Personal Information,
    - to notify the Responsible Party as soon as reasonably possible in the case of a security compromise, and
    - to take any additional steps the Responsible Party requires to comply with the Code;
- comply with the transborder information flows section of the Code where Personal Information is transferred to a Third Party in another country.

6. Perform a personal information impact assessment

A Personal Information Impact Assessment (PIIA) aims to measure current or planned Direct Marketing Activities against the conditions for the lawful Processing of Personal Information set out below.

DMASA members must assess all Direct Marketing Activities against the following conditions.

[15] POPIA regulation 4(c).

[16] POPIA regulation 4(b).

[17] POPIA Regulations 4(e).

6.1. Condition 1: Accountability

The Responsible Party is accountable for complying with the Code.[18] Refer to paragraph 5 for guidance on identifying the Responsible Party and any other role players in a Direct Marketing Activity and their responsibilities.

All Responsible Parties must comply with the accountability checklist in paragraph 5.3.

6.2. Condition 2: Processing limitation

6.2.1 Lawfulness

Responsible Parties must perform a PIIA to assess all Direct Marketing Activities against the Code to ensure that the Processing of Personal Information is lawful and reasonable.[19]

6.2.2 Minimality

Personal Information may only be used in Direct Marketing Activities if the Personal Information is adequate, relevant, and not excessive.[20] The purpose of each piece of Personal Information must be documented.[21]

To assess whether Personal Information is adequate, relevant and not excessive, the Responsible Party must consider the following:

- Is it necessary to collect all the Personal Information? Are some pieces of information not needed to achieve the purpose? The least amount of Personal Information must be collected.
- Is there a less intrusive way to Process Personal Information? If less intrusive methods are available, the Responsible must use the least intrusive Processing method.

6.2.3 Consent, justification, and objection

Responsible Parties may only Process Personal Information based on one of the grounds for lawful Processing. Before starting the Direct Marketing Activity, they must identify and document the relevant ground for lawful Processing.

[18] Section 8 of POPIA.

[19] Section 9 of POPIA.

[20] Section 10 of POPIA.

[21] Section 13 of POPIA.

The grounds for the lawful Processing of Personal Information for Direct Marketing include the following:[22]

- the Data Subject consents to the Processing (available for Direct Marketing by any means or communication channel);
- the Data Subject is a customer of the Responsible Party (available for Electronic Direct Marketing);
- Processing protects the legitimate interests of the Data Subject (only available for Direct Marketing done by postal mail, telephone, or in person);
- Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a Third Party to whom the information is supplied (only available for Direct Marketing done by postal mail, telephone, or in person).

The grounds for the lawful Processing of Special Personal Information and the Personal Information of Children are discussed in paragraphs 6.9 and 6.10.

6.2.3.1 When a Responsible Party must ask for Consent

A Responsible Party must ask for a Data Subject's Consent to Process their Personal Information for unsolicited Electronic Direct Marketing.

Electronic Direct Marketing is Direct Marketing using electronic communication, including

- email
- SMS
- fax
- automatic calling machines
- push notifications

direct messaging via social media Direct Marketing is 'unsolicited' if the Data Subject is not already a 'customer' of similar products or services of the Responsible Party.

Consent must be a voluntary, specific, informed expression of will.[23] A Responsible Party may only approach a Data Subject once to ask for their Consent for Electronic Direct Marketing, and the Consent mechanism must comply with the essential elements of Form 4. This means that Responsible Parties do not have to follow Form 4 verbatim. They are:[24]

- full name of the Data Subject who gives Consent;
- the signature or other mode of acceptance of the Data Subject (in person or electronically);
- the date and location where the Consent was given;

---

[22] Section 11 and 69 of POPIA.

[23] Section 1 of POPIA, definition of consent.

[24] POPIA regulation 6.

- the identity and contact information of the Responsible Party;
- the identity, contact information, and signature of the person designated to act on behalf of the Responsible Party (if the Data Subject engages with the Responsible Party on the Responsible Party's channels, these details are not required);
- what goods, products or services will be marketed; and
- the electronic communication channels that will be used.

The Responsible Party must be able to prove that they received valid Consent from the Data Subject.[25] They must keep a record of:[26]

- proof of when and how they obtained Consent;
- Consent wording;
- the information provided to the Data Subject at the time;
- how they informed the Data Subject; and
- their workflow for receiving Consent and withdrawals of Consent.

6.2.3.2 When a Responsible Party do not need to ask for Consent

Responsible Parties do not have to ask for Consent if they

- send Electronic Direct Marketing of their own similar products or services to 'customers',
- can rely on their own or a Third Party's legitimate interests to do Direct Marketing by postal mail, telephone, or in person;[27] or
- protect the Data Subject's legitimate interests by doing Direct Marketing by postal mail, telephone, or in person.[28]

Electronic Direct Marketing to customers

A Responsible Party does not have to ask for prior (opt-in) Consent for Electronic Direct Marketing of its own similar products or services to 'customers'.

A Data Subject will be considered to be the Responsible Party's 'customer' for purposes of Electronic Direct Marketing when the:[29]

- Responsible Party obtained the Data Subject's contact details 'in the context of a sale of a product or service';

---

[25] Section 11(2)(a) of POPIA.

[26] European Data Protection Board *Guidelines on consent 05/2020* paragraph 108, available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[27] Section 11(1)(f) of POPIA.

[28] Section 11 (1)(d) of POPIA.

[29] Section 69(3) of POPIA.

- Responsible Party obtained the contact details for Direct Marketing. To prove this, the Responsible Party must have notified the Data Subject of their intentions through a privacy notice or statement when they collected the contact details;
- Electronic Direct Marketing is for the Responsible Party's 'own similar products or services'; and

Data Subject was given a reasonable opportunity to object, free of charge, to using their contact details when the information was collected and with each subsequent Direct Marketing communication.

Legitimate interests

Responsible Parties may Process Personal Information for Direct Marketing Activities if the Processing protects the Data Subject's legitimate interests or if the Processing is necessary for pursuing the legitimate interests of the Responsible Party or a Third Party to whom the information is supplied.[30] This justification is only available for Direct Marketing done by mail, telephone, or in person.

To rely on their or a Third Party's legitimate interests, the Responsible Party must show that the limitation of the Data Subject's right to privacy is reasonable.[31] The Responsible Party must do a Legitimate Interest Assessment to determine whether Processing will be lawful. A Legitimate Interest Assessment consists of three parts:[32]

- Purpose test: is the Responsible Party pursuing a legitimate interest (i.e. is the purpose legal)?
- Necessity test: is the Processing necessary for that purpose? Is this the least intrusive way of achieving the result required?
- Balancing test: do the Data Subject's interests override the legitimate interests?

6.2.3.3 Right to unsubscribe and withdraw Consent

Data Subjects must always be allowed to unsubscribe or opt out of Direct Marketing.[33] Refer to paragraph 6.8 for more information about the Data Subjects' rights.

6.2.4 Direct collection from the data subject

Responsible Parties must collect Personal Information directly from the Data Subject.[34]

---

[30] Section 11(1)(d) and (f).

[31] Section 36 of the Constitution of South Africa.

[32] The UK Information Commissioner's Office *Guide to the General Data Protection Regulations. Legitimate interests* available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/.

[33] Section 5(e) of POPIA.

[34] Section 12 of POPIA.

6.2.4.1 Exceptions to the direct collection rule

Responsible Parties may collect Personal Information from Third Parties if one of the following exceptions apply:[35]

Exception[36]	How to use this exception
The Personal Information is contained in or derived from a Public Record.	Examples of Public Records[37] include: • the Deeds Registry • Companies and Intellectual Property Commission ('CIPC') records • certain court records The internet is **not** a public record.
The Data Subject deliberately made the Personal Information public.	If a Responsible Party wants to rely on this exception, the Data Subject must have: • made the information public: • published the Personal Information themselves; and • deliberately made the information public.
The Data Subject gave Consent that the Responsible Party could collect the Personal Information from Third Parties.	The Consent must be voluntary, specific, and an informed expression of will. Responsible Parties must inform the Data Subject of the specific Third Parties or categories of Third Parties from whom they will collect the Personal Information.

[35] Section 12(2) of POPIA.

[36] Section 12(2) of POPIA contains additional exceptions that are not relevant to collection for Direct Marketing Purposes.

[37] Section 1 of POPIA defines a 'public record' as 'a record that is accessible in the public domain; and is in the possession of or under the control of a public body (but not necessarily created by the public body)'. Typically, if there is any impediment (e.g., a paywall or a data wall) to the accessibility of the information, the information is not considered 'accessible in the public domain'.

Collection from a Third Party is necessary to maintain the legitimate interests of the Responsible Party or a Third Party.	Responsible Parties must do a Legitimate Interest Assessment to assess whether their interests outweigh the Data Subject's right to privacy.
Collection from a Third Party would not prejudice a legitimate interest of the Data Subject.	Responsible Parties must assess whether the processing would negatively impact the legitimate interests of the Data Subject.

6.2.4.2 Collection from third parties

If a Responsible Party collects Personal Information from a Third-Party source, the Responsible Party must obtain written confirmation from the Third Party that they comply with POPIA.

6.3. Condition 3: Purpose specification

6.3.1 Collect Personal Information for a specific purpose

Responsible Parties must document the specific purpose why they collect Personal Information.[38]

6.3.2 Retention and restriction Records of Personal Information

The Responsible Party may keep Records of Personal Information after the Direct Marketing Activity is concluded if:[39]

- the Record is required for its functions or activities;
- there is a contract between the Data Subject and the Responsible Party that requires the Record to be retained;
- retention is required or authorised by law;
- the Data Subject consented that the Record be retained; or
- the Responsible Party uses the Record for historical, statistical or research purposes and implements additional security measures, for instance pseudonymisation, implementing strict access controls, etc.

Responsible Parties must create and implement a records retention schedule that determines default rules for:

[38] Section 13 of POPIA.

[39] Section 14(1) and 14(2) of POPIA.

- how long the Record should be retained (e.g., until the conclusion of the Direct Marketing campaign and for three years after that); and
- why the Record must be retained (e.g., for analytics, to measure return on investment).

When a retention period ends, the Responsible Party must delete, destroy or de-identify the Personal Information as soon as reasonably possible.[40] If Personal Information is held in the cloud or by a service provider, the Responsible Party must ensure that the Personal Information, and any backups, are securely deleted, destroyed, or permanently de-identified.[41]

6.4. Condition 4: Further processing limitation

When the initial purpose for which Personal Information is processed changes or the Personal Information is used for a 'new' purpose, it is referred to as further Processing. Responsible Parties may only Process Personal Information further if the new purpose is compatible with the purpose for which the Personal Information was collected.[42]

The Responsible Party must assess whether the new purpose is compatible with the original purpose of collection by considering the following:[43]

- **The relationship between the original purpose and the new purpose.** It will be compatible if the new purpose is implied in the original purpose (e.g., a logical next step).
- **The nature of the Personal Information concerned.** If the Responsible Party uses sensitive Personal Information, such as Special Personal Information or the Personal Information of a Child, the test for compatibility with the original purpose is stricter.
- **The consequences of further Processing for the Data Subject.** The Responsible Party must assess both negative and positive consequences of Direct Marketing Activities for the Data Subject. For instance, will the Data Subject's Personal Information be shared with Third Parties? Will the Data Subject's Personal Information be altered or combined with other datasets? Will the Data Subject reasonably expect the new activity?
- **The way the Personal Information was collected.** The Responsible Party must consider the circumstances in which the Personal Information was collected. Did the Responsible Party collect the Personal Information from Third Parties? What information did the Data Subject receive when their Personal Information was

[40] Section 14(4) of POPIA.

[41] Section 14 (5) of POPIA.

[42] Section 15(1) of POPIA.

[43] Section 15(2) of POPIA.

collected? What would a reasonable person expect their Personal Information to be used for based on the context of the collection?

- **Any contractual rights between the Data Subject and the Responsible Party.** The Responsible Party must consider the nature of their relationship with the Data Subject to assess whether further Processing is compatible with the original purpose of Processing. For instance, what is the generally accepted practice in the context, the balance of power between the Responsible Party and Data Subject, and whether the Data Subject could easily object to the Direct Marketing Activity?

When specific requirements are met, the Responsible Party does not have to assess compatibility as described above and would the further Processing of Personal Information automatically be compatible. These requirements are that:[44]

- the Data Subject **Consented** to the new Processing activity;
- the Personal Information is available in or derived from a **Public Record**;[45]
- the **Data Subject deliberately** made the Personal Information **public**; or
- further Processing of the Personal Information is for **historical, statistical or research purposes** and that the Responsible Party ensured that the Personal Information would not be used for any other purpose and the results would not be published in an identifiable form.

6.5. Condition 5: Information quality

Apart from ensuring that the Personal Information the Responsible Parties Process is adequate, relevant and not excessive, Responsible Parties must also take reasonably practicable steps to ensure that the Personal Information is complete, accurate, not misleading and updated where necessary.[46]

To establish what is 'reasonably practicable', the following factors should be considered:

- The **risk to or impact on Data Subjects** when the Personal Information is incorrect. High-risk activities include profiling and automated decision-making.
- The **availability of technical or other measures** to ensure the quality of the Personal Information. If possible, Responsible Parties should provide easy methods where Data Subjects can update their Personal Information.

---

[44] Section 15(3) of POPIA. Section 15(3) contains additional circumstances when further processing will automatically be compatible. Those circumstances are not relevant to Direct Marketing Activities, so we do not list them here.

[45] A 'public record' is a record that is accessible in the public domain and that is in the possession of or under the control of a public body, whether or not it was created by that public body. See the definition of public record in section 1 of POPIA. Information collected from social media accounts or company websites is not 'public records'.

[46] Section 16 of POPIA

- The **cost** of compliance. The cost may be prohibitive or excessive compared to the risk posed to Data Subjects.

6.6. Condition 6: Openness

6.6.1 Document the direct marketing activities

Responsible Parties must maintain a Record of all Direct Marketing Activities and publish a PAIA Manual that describes the:[47]

- purpose of Processing Personal Information;
- categories of Data Subjects and the categories of Personal Information;
- the recipients or categories of recipients to whom the Personal Information may be supplied;
- planned transborder flows of Personal Information; and
- a general description of the information security measures implemented.

6.6.2 Notify data subjects when collecting personal information

Responsible Parties must inform Data Subjects when they collect their Personal Information and if they intend to use it for Direct Marketing Activities.[48]

Responsible Parties do not have to notify Data Subjects if:

- they notified the Data Subject previously and are subsequently collecting the same kind of Personal Information from the Data Subject for the same purpose; and
- the Data Subject gave Consent not to be notified.[49]

The notification must:

- be made before Personal Information is collected, unless this is impossible (e.g., if it is collected from a Third Party), in which case the Data Subject must be notified as soon as reasonably practical after collection;[50]
- contain all the information listed below;[51]
- be clear and concise; and

[47] Section 17 of POPIA and sections 14 and 51 of PAIA.

[48] Section 18 of POPIA.

[49] Section 18(4) of POPIA lists additional exceptions. We do not mention them here because they are not relevant to Direct Marketing Activities.

[50] Section 18(2) of POPIA.

[51] Section 18(1) of POPIA.

- be kept up to date; for instance, if the Processing purpose changes or Direct Marketing channels change, Personal Information will be shared more widely or sent to another country, then these changes must be reflected in the notice.

Privacy notices or statements must inform Data Subjects of the following:

- the Personal Information being collected
- the source of Personal Information is being collected from
- the name and contact details of the Responsible Party
- the purpose for which the Personal Information is being collected
- whether supplying Personal Information is mandatory or voluntary
- the consequences of not supplying the Personal Information
- any particular law requiring or authorising the collection of the Personal Information
- whether the Responsible Party intends to transfer the Personal Information across borders and the level of protection provided
- the recipients or categories of recipients of the Personal Information
- the nature and category of the Personal Information
- the Data Subject's right to rectify incorrect or out-of-date Personal Information
- the Data Subject's right to object to Direct Marketing
- the Data Subject's right to complain to the Regulator, and the Regulator's contact details

6.7. Condition 7: Security safeguards

6.7.1 Establish appropriate technical and organisational safeguards

POPIA provides that a Responsible Party must establish appropriate, reasonable, technical and organisational safeguards to secure Personal Information.[52] When considering what is appropriate, Responsible Parties must identify the risks posed by their Direct Marketing Activities and obtain expert advice (if necessary) to achieve the level of security that is proportionate to the risk to the Data Subject. Responsible Parties must have due regard to generally accepted information security practices and procedures which may apply to Direct Marketing Activities

The following elements could indicate a high-security risk in Direct Marketing Activities:

- large-scale Processing
- matching or combining Personal Information from different sources
- Processing Special Personal Information
- Processing Personal Information of Children or other vulnerable groups
- where Processing may give rise to discrimination, identity theft or fraud
- sharing Personal Information across borders
- sharing Personal Information with Third Parties

[52] Section 19(1) of POPIA.

- using new or unusual technologies

6.7.2 Security compromises

This section applies to 'security compromises' where there are reasonable grounds to believe that Personal Information has been accessed or acquired by an unauthorised person.[53]

Responsible Parties must ensure that their employees are trained to recognise and report security compromises.

Responsible Parties must document a security compromise response procedure and have an email address or telephone number where anyone can report a suspected security compromise. The security compromise procedure must include the following steps:

- mitigate risks as soon as reasonably practicable by restoring the confidentiality, integrity and availability of Personal Information and preserving evidence;
- conduct a risk assessment by identifying the possible consequences of the security compromise and identifying measures the Responsible Party and Data Subjects can take to mitigate consequences and to protect Data Subjects from further unauthorised access;
- notify the Regulator using Form SCN1 as soon as reasonably possible after discovering the security compromise, taking into account the requirements of law enforcement and any measures reasonably necessary to mitigate the risks to the Responsible Party and Data Subjects; and
- notify Data Subjects as soon as reasonably possible after discovering the security compromise unless a Public Body in law enforcement or the Regulator asks for a delay.

Responsible Parties must notify Data Subjects of a security compromise in at least one of the following ways, namely by:

- mail at the last known physical or postal address;
- email;
- SMS;
- placing a prominent notice on the Responsible Party's website; or
- publishing a notice in the news media.

6.8. Condition 8: Data subject participation

In terms of POPIA, Data Subjects have certain rights regarding Direct Marketing. Responsible Parties must ensure that Data Subjects can exercise these rights and that the procedure Data Subjects should follow is effortless and free.

[53] Section 22(1) of POPIA.

6.8.1 The right to unsubscribe from direct marketing communications

Data Subjects always have the right to unsubscribe from Direct Marketing. Data Subjects may unsubscribe directly with the Responsible Party.[54]

Responsible Parties must include the following in all Direct Marketing communications to Data Subjects:

- 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 Data Subject may send a request that Direct Marketing must cease.[55]

The unsubscribe process must be free of unnecessary formality. [56]

In certain circumstances the unsubscribe process must be free of charge, for instance:

- when determining whether a Data Subject is a 'customer' for Electronic Direct Marketing purposes (see paragraph 6.2.3.2), the Data Subject must have been given a reasonable opportunity to object free of charge when the Personal Information was collected and each with each Direct Marketing communication thereafter;
- when the Data Subject counts as a 'consumer' as defined in terms of the Consumer Protection Act[57]; and
- when the Responsible Party is a member of the WASPA Code of Conduct.[58]

[54] Section 5(e) of POPIA.

[55] Section 69(4) of POPIA.

[56] Section 69(3) of POPIA.

[57] 68 of 2000 ('the CPA'). Section 11(2) of the CPA provides that 'to facilitate the realisation of each consumer's right to privacy, and to enable consumers to efficiently protect themselves against the activities contemplated in subsection (1), a person who has been approached for the purpose of direct marketing may demand during or within a reasonable time after that communication that the person responsible for initiating the communication desist from initiating any further communication', Additionally, section 11(5) provides that 'No person may charge a consumer a fee for making a demand in terms of subsection (2) or registering a pre-emptive block as contemplated in subsection (3)'. Therefore, read together, sections 11(2) and 11(5) of the CPA require that unsubscribe processes for direct marketing sent to 'consumers' under the CPA, must be free of charge.

[58] Section 16.7 of the WASPA Code of Conduct states that ' A member may not charge a consumer a fee for processing an opt-out request or for registering a pre-emptive block'.

Responsible Parties must process unsubscribe requests promptly. Where possible, the Responsible Party must offer the unsubscribe method through the same communication channel on which the Data Subject received the Direct Marketing.[59]

6.8.2 The right to withdraw Consent

Data Subjects have the right to withdraw Consent for any Direct Marketing at any time.[60] When they do, the Responsible Party must stop Processing the Personal Information for Direct Marketing.

6.8.3 The right to access their Personal Information

Data Subjects have a right to know that their Personal Information is being used in Direct Marketing Activities and to access a Record of their Personal Information. Data Subjects may also ask which Third Parties have had access to their Personal Information.[61]

Responsible Parties must implement procedures to ensure that they can verify the identity of Data Subjects and respond to the requests of Data Subjects:[62]

- within a reasonable time;
- in a reasonable manner and format; and
- in a reasonably understandable form.

The right to access Personal Information is not absolute. Responsible Parties may or must refuse to disclose information to which the grounds for refusal set out in Chapter 4 of Part 2 and Chapter 4 of Part 3 of PAIA apply. For instance, Data Subjects are not entitled to their own Personal Information if giving access would:

- reveal the Personal Information of someone else without the other person's permission;[63]
- disclose privileged documents (in the context of legal proceedings) unless the person entitled to the privilege has waived that privilege;[64]

---

[59]Federation of European Direct and Interactive Marketing's ('FEDMA's) 'European Code of Practice for the use of personal data in direct marketing electronic communications annex' on page 7, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp174_annex_en.pdf

[60] Section 11(2)(b) of POPIA.

[61] Section 23(1) of POPIA.

[62] Section 23(1)(b) of POPIA. The prescribed forms and applicable fees are prescribed by the PAIA regulations of 2021 available at https://inforegulator.org.za/acts/.

[63] Section 34 or 63 of PAIA.

[64] Section 40 or 67 of PAIA.

- endanger the life or safety of an individual;[65]
- breach the Responsible Party's contractual duty of confidence owed to a Third Party;[66] or
- compromise someone else's intellectual property or confidential information.[67]

If a part of the Personal Information requested may or must be refused, the Responsible Party must disclose every other part of the information.

6.8.4 The right to correct or delete personal information

Data Subjects may ask a Responsible Party to:[68]

- correct inaccurate, out-of-date, incomplete, or misleading Personal Information that it possesses or controls;
- delete excessive, irrelevant, out-of-date, incomplete, misleading, or unlawfully obtained Personal Information that it possesses or controls; and
- destroy or delete Personal Information it controls in contravention of this Code.

When Responsible Parties receive such a request they must first verify the identity of the Data Subject, and then they must either:[69]

- correct, delete, or destroy the Personal Information; or
- provide credible evidence of the accuracy and validity of the Personal Information to the satisfaction of the Data Subject (in the interim, use of the Personal Information must be restricted).[70]

If the Responsible Party and Data Subject cannot agree on whether the Personal Information is accurate, the Responsible Party must indicate in their records that the Personal Information is disputed.[71]

If the Responsible Party agrees that the Personal Information should be corrected or deleted and if the correction or deletion will impact decisions that have been or will be

---

[65] Section 38 or 66 of PAIA.

[66] Section 37 or 65 of PAIA.

[67] Sections 36, 37, 42, 64, 65 or 68 of PAIA.

[68] Section 24(1) and Regulation 3 of POPIA.

[69] Section 24(2)(a) to (c) read with section 14(6)(a) of POPIA.

[70] Section 14(4)(a) of POPIA.

[71] Section 24(2)(d) of POPIA.

taken about Data Subjects, the Responsible Party must inform everybody who had access to or who were provided with the Personal Information about the correction or deletion.[72]

6.8.5 The right to make representations about automated decisions with a legal or substantial effect

Data Subjects have additional rights if the Direct Marketing Activities involve automated decision-making. Automated decisions are decisions that:[73]

- have legal consequences or will have a substantial effect on the Data Subject;
- are automated (i.e., made without human intervention); and
- are based on an analysis of aspects of the Data Subject's personality, behaviour, interests, and habits (e.g., creditworthiness, location, personal preferences, or conduct).

When Direct Marketing Activities involve automated decision-making, Responsible Parties must:[74]

- allow Data Subjects to make representations about the decision; and
- provide Data Subjects with sufficient information about the underlying logic of the automated decision to allow them to make representations.

6.9. Processing Special Personal Information

One of the following justifications must apply if a Responsible Party wants to Process Special Personal Information in Direct Marketing Activities:[75]

- the Personal Information was deliberately made public by the Data Subject;[76]
- the Data Subject consented to the Processing of their Special Personal Information for the Direct Marketing Activities;[77] or
- a justification provided in sections 28 to 33 applies.[78]

---

[72] Section 24(3) of POPIA.

[73] Section 71(1) of POPIA.

[74] Section 71(2)(b) and 71(3) of POPIA.

[75] Section 27 provides for additional justifications for the use of Special Personal Information. We do not mention them here because they do not apply to Direct Marketing Activities.

[76] Section 27(1)(e) of POPIA.

[77] Section 27(1)(a) of POPIA.

[78] Section 27(1)(f) of POPIA.

6.10. Processing Personal Information of Children

One of the following justifications must apply if a Responsible Party wants to Process the Personal Information of Children in Direct Marketing Activities:

- the Personal Information was made public deliberately by the Child with the Consent of a parent or guardian;[79] or
- a parent or guardian Consented to the Child's Personal Information being used for Direct Marketing.[80]

If a Responsible Party wants to Process the Special Personal Information of a Child for Direct Marketing Activities, they must also comply with the requirements for the lawful Processing of Special Personal Information.

6.11. Transborder information flows

Direct Marketing Activities often require the transfer of Personal Information to other countries. A Responsible Party in South Africa may not transfer Personal Information to a Third Party who is in a foreign country unless:[81]

- the Third-Party recipient is subject to a law, Binding Corporate Rules or binding agreement which provide an adequate level of protection that
    - effectively upholds the principles for reasonable Processing of the information that is substantially similar to the conditions for lawful Processing of Personal Information in POPIA; and
    - includes provisions that are similar to this paragraph, relating to the 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;
- the transfer is necessary for the implementation of pre-contractual measures taken 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; or
- the transfer is to the benefit of the Data Subject, but it was impossible to obtain their Consent, and they would likely have Consented to the transfer if asked.

---

[79] Section 35(1)(e) of POPIA.

[80] Section 35(1)(a). Section 35 provides for additional justifications for the use of the Personal Information of Children. We do not mention them here because they don't apply to Direct Marketing Activities.

[81] Section 72(1) of POPIA.

6.12. Information matching programmes

Information Matching Programmes form a vital part of the Direct Marketing industry, mainly concerning Direct Marketing Activities such as data enrichment, Profiling, and Lead Generation.

Example of an Information Matching Programme in a Direct Marketing context:

DMASA members must de-duplicate their Direct Marketing campaign lists against DMASA's Do Not Contact (DNC) register. Members must compare the Data Subjects' contact details in their campaign databases with those on the DNC register to see whether any Data Subjects in their databases have registered.

Responsible Parties who use Information Matching Programmes must put adequate safeguards in place In addition, they must:

- ensure that the algorithms used to match the information have been validated and reviewed to ensure that the information is valid, applicable, fair, and appropriate;
- put measures in place to regularly assess the quality of the Personal Information used in the Information Matching Programme; and
- provide Data Subjects whose Personal Information is used in the programme meaningful access to the Personal Information and allow Data Subjects to make representations about the accuracy of the information unless prohibited by law.

6.13. Profiling and automated decision-making

Marketing profiles are records of Data Subject's characteristics created by acquiring Personal Information from multiple sources and then using it to target products and services.[82]

Profiling has two components, namely:

- profile generation: the process of inferring a profile;[83] and

profile application: the process of treating (i.e., deciding on a person or entity) Data Subjects in light of this profile.[84]If a Responsible Party makes automated decisions based on Profiles that result in legal consequences for the Data Subject or that substantially affect the Data

[82] SA Law Reform Commission Project 124 on Privacy and Data Protection (2009 Report), page 367, available at https://www.saflii.org/za/other/ZALRC/2009/1.pdf.

[83] Section 71(1) of POPIA includes a list of examples that would be considered as 'profiling' including profiles created to assess the data subject's 'performance at work, or his, her or its creditworthiness, reliability, location, health, personal preferences or conduct'.

[84] SA Law Reform Commission Project 124 on Privacy and Data Protection (2009 Report), page 368, available at https://www.saflii.org/za/other/ZALRC/2009/1.pdf.

Subject, the Responsible Party must implement appropriate measures to protect the Data Subject's legitimate interests, including to:

- provide an opportunity for the Data Subject to make representations about the decision; and
- provide the Data Subject with sufficient information about the underlying logic of the automated Processing of the information and allow Data Subjects to make representations about the accuracy of the information unless prohibited by law.

7. Authorisations

The Regulator has issued this Code in terms of chapter 7 of POPIA after DMASA applied on behalf of their members. This means that DMASA members who Process Personal Information for Direct Marketing Activities in compliance with this Code are exempt from:

- requesting prior authorisation for the processing activities referred to in section 57(1) of POPIA;[85] and
- having to notify the Regulator when they intend to conduct any Processing activities as referred to in section 57(1) of POPIA.[86]

This includes an exemption for activities that involve the Processing of unique identifiers for purposes other than the purpose it was initially collected for, to link, pool or combine the Personal Information with the Personal Information Processed by other Responsible Parties.[87]

Some linking activities of unique identifiers will constitute an Information Matching Programme, and some will not. Even though Responsible Parties regulated by this Code are not required to notify the Regulator or obtain prior authorisation for linking activities involving unique identifiers, linking activities are still considered 'high-risk'.[88] This means that Responsible Parties conducting linking activities involving unique identifiers must

---

[85] The specific processing activities include: processing any unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection, and with the aim of linking the information together with information processed by other responsible parties; processing information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties; processing information for credit reporting; and transferring special personal information, or the personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information (section 57(1) of POPIA).

[86] Section 58 of POPIA.

[87] Section 57(1)(a) of POPIA.

[88] ICO 'Examples of processing 'likely to result in high risk', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

implement the same safeguards as required for Information Matching Programmes in paragraph 6.12.

8. Enforcement of the Code

The following people may submit a complaint in terms of this Code:

- a Data Subject
- a person acting on behalf of a Data Subject
- a competent person acting on behalf of a Data Subject who is a Child

Responsible Parties and DMASA must follow the following process when they receive a complaint from a Data Subject:

8.1. The data subject must complain to the responsible party first

Responsible Parties must:

- let Data Subjects know how to complain;
- use a complaint form that is substantially similar to Part 1 of Form 5;[89]
- have a dedicated team or channel to receive complaints and make the contact details of this team or channel readily available to Data Subjects ;
- have a process in place to manage complaints; and
- help Data Subjects to ensure that the complaint is heard – even if Data Subjects do not follow the correct procedure.

If a Data Subject believes that a Responsible Party has breached this Code, they must first complain to the Responsible Party, where appropriate and practical.[90] If a Data Subject makes the complaint directly with DMASA, DMASA will refer the complaint to the Responsible Party.

Data Subjects or DMASA may escalate the complaint to the Regulator if:

- the Data Subject will be disadvantaged if the complaint is directed to the Responsible Party;
- a systemic violation of the protection of Personal Information has occurred;
- the Responsible Party has a history of habitual violation of the Code;
- the complainants represent a class of Data Subjects that brings a complaint against the same Responsible Party; or
- several complaints have arisen from similar circumstances, and there is a common issue of law or fact.

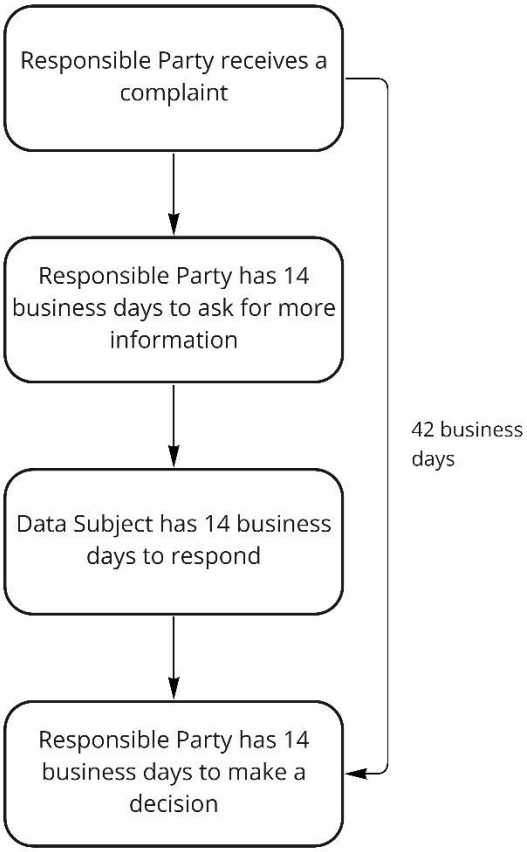
[89] POPIA regulation 7.

[90] Section 77(1)(f) provides that the Regulator can decline to act if the data subject does not follow the complaints procedure set out in an accredited Code.

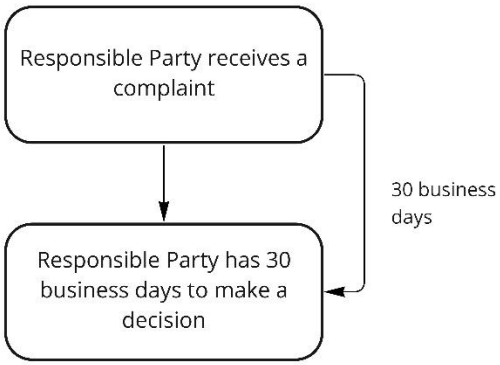
8.2. The responsible party must investigate the complaint

If the Responsible Party needs further information to investigate the complaint, they must request it from the Data Subject within 14 business days of receiving the complaint.

They must give the Data Subject at least 14 business days to respond. The Responsible Party must decide on the information received from the Data Subject within 14 business days of the end of the response period. The Responsible Party must provide reasons for their decision in writing and in plain language.



However, if the Responsible Party does not require further information from the Data Subject, the Responsible Party must decide within 30 business days of receiving the complaint.



Throughout the complaint process, the Responsible Party must keep the Data Subject adequately informed of:

- the progress of the complaint;
- causes of any delays in the finalisation of the complaint and revised timelines;
- the Responsible Party's decision in response to the complaint; and
- the reasons for the Responsible Party's decision in response to the complaint.

8.3. The data subject may escalate the complaint to DMASA

If the Data Subject is unsatisfied with the Responsible Party's decision, the Responsible Party must inform the Data Subject of their right to escalate their complaint to DMASA. The Responsible Party must provide reasonable assistance to ensure that the Data Subject's complaint reaches DMASA.

The Data Subject may escalate the complaint to DMASA within 30 business days of receiving the Responsible Party's decision.

The Data Subject must send the following documentation to the DMASA Complaints Department via email at complaints@dmasa.org or via post or in person to Fernridge Office Park, Block 4 Ground Floor, 5 Hunter Street, Ferndale, Johannesburg, 2193:

- the original complaint and any additional information they provided to the Responsible Party and the date of the complaint
- the decision made by the Responsible Party and the date of the decision
- the reasons why the Data Subject disagrees with that decision

8.4. DMASA must facilitate the complaint

DMASA must facilitate the hearing of all complaints escalated to them in terms of the Code. DMASA may facilitate complaints escalated to them in terms of this Code, either by way of an assessment, or an investigation of the complaint.

8.4.1 Assessment

DMASA may, to settle the complaint speedily, assess the merits of the complaint without doing an investigation and suggest to the Data Subject and Responsible Party how the complaint should be settled.

DMASA may, after collecting relevant records and information to assess the complaint, form an initial view on the matter with respect to:

- the Responsible Party's potential liability; and
- the remedies (if any), DMASA believes the Data Subject is entitled to.

The possible outcomes of an assessment include:

- the complaint is resolved as requested by the Data Subject; or
- some, but not all remedies requested by the Data Subject are provided; or
- none of the remedies requested by the Data Subject are provided, and DMASA suggests other remedies available to the Data Subject.

8.4.2 Investigation

DMASA may investigate the complaint. DMASA representatives may engage directly with the Responsible Party and the Data Subject to try and resolve the complaint.

If the Responsible Party assures DMASA that they will not repeat the action that the complaint was about, and the Data Subject is satisfied, DMASA may facilitate a settlement agreement between the Responsible Party and the Data Subject.

8.4.3 Mediation

DMASA mut advise the Responsible Party and the Data Subject of its decision regarding the assessment or investigation within 30 business days of receiving the complaint.

The Responsible Party and the Data Subject must advise the DMASA within 10 business days of receiving DMASA's decision about whether they accept DMASA's decision or not.

If the complaint is resolved because of the Responsible Party and the Data Subject accepting DMASA's decision or acquiring DMASA's assistance in arriving at a settlement agreement, the decision must be recorded and carried out.

If the Responsible Party or Data Subject do not accept DMASA's decision or cannot arrive at a settlement agreement and the complaint remains unresolved, DMASA must inform the Responsible Party and the Data Subject of the further options available to them (including referring the complaint to the independent adjudicator, referring the complaint to the Regulator or instituting civil proceedings).

8.5. The independent adjudicator reviews the decision

If DMASA cannot broker a settlement agreement or provide a decision which both the Responsible Party and Data Subject accept within 45 business days of receiving the complaint, it will refer the complaint to the independent adjudicator(s) and provide them with all the documents that the Responsible Party and the Data Subject submitted. The independent adjudicator(s) may ask the Responsible Party and the Data Subject for more information. The adjudication of the complaint by an independent adjudicator will take place in Johannesburg and in accordance with the rules of the Arbitration Foundation of Southern Africa's domestic arbitration rules. These rules can be found at https://arbitration.co.za/.

The independent adjudicator(s) must provide DMASA with a written decision on the complaint within 45 business days of receiving the complaint. It may take longer if it is necessary to ask for more information to adjudicate the complaint fairly. If the independent adjudicator(s) finds that the Responsible Party is in breach of the Code, DMASA may ask the Responsible Party to:

- take specified steps; or
- stop Processing Personal Information for a specified purpose or in a specified manner.

DMASA will communicate the decision to the Responsible Party within 14 business days of receiving the independent adjudicator's decision.

8.6. The data subject or responsible party may refer the complaint to the Regulator

If the Responsible Party or the Data Subject is dissatisfied with the independent adjudicator's decision, they may refer the complaint to the Regulator. They can do this by submitting Part II of Form 5 to POPIAcomplaints@inforegulator.org.za within 30 business days of receiving the decision.[91]

The independent adjudicator's decision will remain in effect until the Regulator makes a decision.[92]

8.7. The data subject may institute civil proceedings

Regardless of where they are in the complaints process, the Data Subject may institute civil proceedings regarding an alleged interference with the protection of their Personal Information (as provided for in terms of section 99 of POPIA) at any time.

---

[91] Section 63(3) of POPIA and POPIA Regulation 7.

[92] Section 63(4) of POPIA.

9. Independent adjudicator

9.1. Appointment

DMASA must appoint one or if it deems necessary, more than one independent adjudicators. Individuals appointed by DMASA as independent adjudicators must have suitable qualifications or experience at an expert level in the legal and Direct Marketing industry. They must have an impeccable reputation and must not have been found guilty of misconduct or ethical violations in the past.

When DMASA receives a complaint for adjudication, DMASA must assign an independent adjudicator(s) to make a decision. The assigned independent adjudicator(s) must not have any conflicts of interest or any affiliation with the Responsible Party or Data Subject.

9.2. How independent adjudicators must adjudicate complaints

The independent adjudicator must:

- consider the matters listed in section 44 of POPIA when adjudicating a complaint;
- be impartial;
- be accessible and efficient;
- assist Data Subjects in participating in the adjudication process;
- follow a flexible procedure; and
- observe the principles of natural justice and procedural fairness.

Adjudicators may call for further information or require that the Data Subject or Responsible Party provide oral evidence.

9.3. Reports to the Regulator

The panel of independent adjudicators must submit an annual report to the Regulator that specifies the number and nature of complaints made to the panel during that financial year.

The report must be made in a form satisfactory to the Regulator within five months of the end of the Regulator's financial year (31 March).

10. Administration of the Code

DMASA may, on its own or in response to a complaint:

- ask a Responsible Party to demonstrate their compliance with the Code by producing the documentation referred to in the accountability checklist at paragraph 5.3; and
- require a Responsible Party to produce a report by an independent auditor on their compliance with the Code at the cost of the Responsible Party.

DMASA will provide an annual report to the Regulator. This report must include:

- the steps DMASA took to monitor compliance with the Code;

- information received from Responsible Parties on their level of compliance;
- the number and nature of complaints made to an adjudicator during that financial year, the average time it took to resolve the complaints and statistical information about the nature and outcomes of the complaints;
- aggregate information about systemic issues or serious or repeated non-compliance with the Code; and
- trends on the effectiveness of the Code.

11. Review and expiry of the Code

11.1. Review

DMASA may review the Code annually and apply for the Regulator's approval for any amendments resulting from a review. [93]

If the Regulator has approved the amended Code, DMASA will publish the amended Code on its website within 14 business days from the date of publication of the amended Code in a Government Gazette.

The Regulator may also, on its own initiative, review the operation of the Code at any time. If the Regulator deems it necessary, the Regulator may also amend or revoke the Code with immediate effect or at a future date to be determined by the Regulator.

11.2. Expiry

Unless revoked by the Regulator, the Code will terminate on the last day before the 5th anniversary of the commencement date. DMASA may apply to the Regulator for the issue of a revised or new Code before the expiry of the current Code.

12. Glossary

Binding Corporate Rules	Binding Corporate Rules are 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 undertakings. A group of undertakings means a controlling undertaking and its controlled undertakings.

[93] Section 64 of POPIA, read with sections 30-34 of the Guideline to Develop Codes of Conduct in terms of Section 65 of the Protection of Personal Information Act, 2013 (No.4 of 2013).

Child	A natural person under 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself
Competent Person	Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the Processing of personal information
Data Subject	The person to whom personal information relates
De-identify	In relation to personal information of a data subject, de-identify means to delete any information that— (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject, and "de-identified" has a corresponding meaning
Direct Marketing	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
Direct Marketing Activities	Includes all the activities in the direct marketing process that involve the Processing of personal information. For instance: • collecting Personal Information for Direct Marketing • lead generation for Direct Marketing • profiling Data Subjects for purposes of Direct Marketing • sending Direct Marketing messages • telemarketing • managing Data Subjects' Direct Marketing consent • asking Data Subjects for donations • destroying or deleting Personal Information used for Direct Marketing
DMASA	The Direct Marketing Association of South Africa

Electronic Communication	Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or the recipient's terminal equipment until it is collected by the recipient
Electronic Direct Marketing	Direct marketing by means of electronic communication. For instance: • email • SMS • fax • automatic calling machines • push notifications • direct messaging via social media
Information Matching Programme	The comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject
Information Officer	Of, or in relation to, a— (a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or (b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act
Lead Generation	Identifying and cultivating Data Subjects as potential customers for products or services.
Legitimate Interest Assessment	A balancing test of the Responsible Party or Third Party's interest against the Data Subject's rights and interests.
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
Person	A natural person or a juristic person

Personal Information	Information relating to an identifiable, living, natural person, and where it is 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, email 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 if the disclosure of the name itself would reveal information about the person
Personal Information Impact Assessment/PIIA	An assessment which is used to assess whether a process complies with POPIA.
Processing	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
PAIA	The Promotion of Access to Information Act 2 of 2000 and its regulations
POPIA	The Protection of Personal Information Act 4 of 2013 and its regulations
Profiling	Means any form of automated Processing of Personal Information to evaluate certain aspects relating to a Data Subject.

Public body	Means- (a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when- (1) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or (2) exercising a public power or performing a public function in terms of any legislation.
Public Record	A record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body
Record	Any recorded information— (a) regardless of form or medium, including any of the following: (i) writing on any material; (ii) 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; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence
Regulator	The Information Regulator established in terms of section 39 of POPIA.[94]
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

[94] More information about the Regulator is available on their website https://inforegulator.org.za/.

Special Personal Information	Personal information concerning— (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or (b) the criminal behaviour of a data subject to the extent that such information relates to— (i) the alleged commission by a data subject of any offence; or (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings
Third Party	Means a natural or legal person, Public Body, agency or body other than • the Data Subject, • Responsible Party, • Operator, and • persons who, under the direct authority of the Responsible Party or Operator, are authorised to process personal information.
Unique Identifier	Any identifier that is assigned to a data subject and is 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