

POPIA FAQ

1.

POPIA AND DIRECT MARKETING

The Protection of Personal Information Act (POPIA) will come into effect on 1 July 2021 and it has a direct impact on the direct marketing industry. Due to it being a new piece of legislation and there being no case law on how to interpret and apply these sections, there are lots of questions in the industry on what it actually means for them.

It is impossible to give 100% clarity at this stage, seeing as we would need to see how the Information Regulator and the Courts eventually interpret the relevant sections, but we have spoken to privacy lawyers to get their views on some of the main questions members have at the moment. This document explains some views on how these sections could be interpreted and provides some guidance on how to comply with POPIA. It is important to note, that this could change in the future, but we are working to stay on top of all developments in this field and will continue to update members of any changes that are relevant to them.

1.1 Does telemarketing fall within s69?

Will POPIA allow us to still dial consumers directly?

In short, no telemarketing does not fall within section 69 of POPIA because it is not 'electronic communication' as defined in section 1 of POPIA.

One of the most important definitions in POPIA is 'electronic communication.' If direct marketing is done 'by means of electronic communication,' the consent requirements in section 69 will apply. In POPIA, it is defined as 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.¹ Section 69(1) provides that electronic communication includes automatic calling machines, facsimile machines, SMSs or email.

The South African definition has three elements:

- any text, voice, sound or image message,
- sent over an electronic communications network,²
- which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.³

For section 69 to apply, all three elements of the definition of electronic communications network must apply. For example, it is not enough that a message is sent over an electronic communications network; the message must also be stored in the network until it is collected by the data subject.

This is how the definition of 'electronic communication' applies to different marketing channels:

Electronic communication



Automatic calling machines

Automatic calling machines are specifically mentioned in section 69(1) as a form of electronic direct marketing. Section 69(5) refers to 'automated calling systems without human intervention.' This would not include automatic diallers that connect to a call centre agent but would include so-called robocalls where the data subject hears a recorded message. The reason why the stricter rules of section 69(3) apply is that it is impossible for the data subject to opt out during the call as there is no simultaneous participation between the data subject and the marketer.⁴

The definition of 'electronic communication' requires that a message must be 'stored in the network or in the recipient's terminal equipment until it is collected by the recipient.' The definition of electronic communication in section 1 of POPIA was based on the definition of 'electronic mail'

Not Electronic communication



Telephone calls, whether transmitted through mobile networks, fixed networks or voice over internet protocols

Direct marketing done via the telephone is not subject to section 69 regardless of whether the call is placed via a mobile network, fixed network or voice over internet protocols. This is because the message is not stored in the network or in the recipient's terminal equipment until it is collected by the recipient.⁵

A close examination of the South African Law Reform Commission's Report reveals that it was a calculated decision based on a strategic decision made by the Department of Trade and Industry to promote call centres within South Africa and to offer incentives to attract call centre business to South Africa⁶ and the role of telemarketing in ensuring that vulnerable

¹ See the definition of 'electronic communication' in section 1 of POPIA.

² The Electronic Communications Act 36 of 2005 provides the following definition for 'electronic communications network' in section 1: 'any system of electronic communications facilities (excluding subscriber equipment), including without limitation— (a) satellite systems; (b) fixed systems (circuit- and packet-switched); (c) mobile systems; (d) fibre optic cables (undersea and land-based); (e) electricity cable systems (to the extent used for electronic communications services); and (f) other transmission systems, used for conveyance of electronic communications.'

³ See the definition of 'electronic communication' in section 1 of the POPIA.

⁴ South African Law Reform Commission *Project 124 Privacy and Data Protection Report*, page 360. The report is available at https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf.

⁵ Does 'electronic communication' under POPIA also refer to so-called 'display ads' or behavioural advertising using targeted social media marketing or tracking cookies? This is a tricky, tricky area indeed! It is very complicated, and to be honest, we are not 100% sure ourselves. The EU Article 29 Data Protection Working Party doesn't think so. See EU Article 29 Data Protection Working Party 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' at 20 to 21, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140. Also see European Data Protection Board 'Guidelines 8/2020 on the targeting of social media user' at para 31 available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en on social media marketing and who is accountable.

⁶ Page 357. Be sure to read footnote 102, it is very interesting.

Electronic communication



in the Directive on privacy and electronic communications.⁷ The requirement that a message must be stored did not apply to 'automatic calling machines' in the Directive, but only to electronic mail. In POPIA, the requirement is included in the definition of electronic communication and 'automatic calling machines' is listed as an example of an electronic communication. This means that automatic calling machines would only be subject to section 69 if a message is left for the data subject to retrieve.



Facsimile

The Mail and Guardian eloquently asks, 'Who the fax is still sending faxes?'¹⁰ Wikipedia says that roughly 2% of marketers (in the United States) still use fax, mostly for business-to-business marketing.¹¹

As with automated calling machines, the inclusion of 'facsimile' as an example of an electronic communication is strange, because the message is not 'stored in the network or in the recipient's terminal equipment until it is collected by the recipient' unless the marketer is making use of fax to email (for instance).



SMS



Email



Push notifications or direct in-app messages (e.g., a 'DM' on social media)

The EDPB and the UK's ICO think confirms that the marketing delivered via a direct in-app message (e.g., a direct message or 'DM' on Instagram or LinkedIn) or a push notification to the user constitutes 'electronic direct marketing.'¹² This is in keeping with the South African definition of 'electronic communication'.

Not Electronic communication



consumers have access to goods and services.⁸ The Commission recommended that 'a regulatory framework for direct marketing be promoted that will balance the rights of consumers not to be targeted unreasonably, with the right of business to communicate effectively with the public.'⁹ The result was an opt-in regime for unsolicited electronic marketing, which would operate alongside the opt-out regime in the Consumer Protection Act 68 of 2008 (the CPA) for other forms of marketing.



Snail mail

Marketing delivered via mail is not subject to section 69 of POPIA. When this marketing is directed at a 'consumer', the CPA will apply.



Targeted social media marketing and behavioural advertising

Social media platforms allow responsible parties to create an 'audience' out of the social media platform's users to display adverts to these users about whichever goods and services in question. Sometimes, the responsible party will send personal information it already has (e.g., email addresses) to the social media platform, and they will match it to their users. This is sometimes referred to as list-based targeting tools. In other instances, social media platforms will offer responsible parties the ability to build an audience based on desirable demographics or preferences. This is referred to as a 'lookalike audiences'. Once the audience has been identified, advertising will be displayed to members of that audience.

Similarly, behavioural advertising allows marketers to display relevant advertising on websites. In this case, the audience is selected based on their web browsing behaviour, which is tracked through the use of cookies.

⁷ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

⁸ Page 360.

⁹ Page 362. The Constitutional right to freedom of expression included the freedom to 'impart information' (section 16(1)(c)(iv)). In addition, section 22 establishes the right to choose a trade, occupation or profession and section 32 establishes the right to access to information. The SALRC balanced these rights with the right to privacy and added that 'it is important to note that it is widely recognised by political and economic commentators that economic growth is essential for the realisation of social and economic transformation in South Africa. Fair marketing practices designed to approach, inform and retain customers must accordingly be regarded as of critical importance to the growth of the South African economy.

¹⁰ Available at: <https://mg.co.za/article/2018-01-19-00-who-the-fax-is-still-sending-faxes/>

¹¹ https://en.wikipedia.org/wiki/Direct_marketing#Broadcast_faxing

¹² The EDPB and the UK's ICO think that the marketing must be delivered via a direct in-app message (e.g. a direct message or 'DM' on Instagram or LinkedIn) or a push notification to the user, to constitute 'electronic direct marketing'. ICO 'Direct marketing: code of practice, Information Commissioner's Office Draft code for consultation' page 16 and 90 available at: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-direct-marketing-code-of-practice/>. Given that POPIA's definition of 'electronic communication' is almost word-for-word identical to the ePrivacy Directive's definition of 'electronic mail', we think it is safe to apply the findings of the EDPB in a South African context as well.



Not Electronic communication



Does 'electronic communication' under POPIA include social media marketing where the marketing is not sent to the data subject, but rather displayed? The EDPB states that '[t]he use of the word "sent" implies the use of technological communication means that necessarily involve the conveyance of a communication, whereas most advertising on the web (through social media platforms or on websites) would not involve "sending" advertisements in the strict sense.¹³ In other words, this form of marketing does not fall within the definition of 'electronic communication', because the marketing is not 'sent' and a message is not 'stored in the network or in the recipient's terminal equipment until it is collected by the recipient.'

To summarise, telemarketing, snail mail, some forms of social media marketing and behavioural advertising (e.g., facilitated by tracking cookies) are not considered 'electronic' and is not subject to section 69 of POPIA. This means that these forms of marketing must be justified in terms of section 11. Responsible parties could argue that marketing their products and services are in the 'legitimate interest of the responsible party.'¹⁴ If a

responsible party wants to rely on this legal basis, it must perform a legitimate interest assessment to ensure that the limitation of the right to privacy is justified. When a responsible party relies on its legitimate interest to market, the data subject will have a right to object (i.e., unsubscribe). In addition, when the data subject is also a 'consumer', the right to unsubscribe to direct marketing in terms of the CPA will apply.



¹³ See EU Article 29 Data Protection Working Party 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' at 20 to 21, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140. Also see European Data Protection Board 'Guidelines 8/2020 on the targeting of social media user' at para 31 available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_en on social media marketing and who is accountable.

¹⁴ Article 29 Data Protection Working Party *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC*.

1.2 Will we be allowed to SMS consumers regarding financial offerings?

The General Code of Conduct for Authorised Financial Services Providers and Representatives (Code) sets out the rules for direct marketing and advertising for financial service providers and their representatives. The Code was amended recently.¹⁵ These amendments to the Code amended the definitions of advertising and direct marketing and creates an opt-out system for 'unwanted direct advertising.'¹⁶

The Code defines 'direct marketing' as 'the rendering of financial services by way of telephone, Internet, digital application platform, media Insert, direct or electronic mail but excludes the publication of an advertisement.'¹⁷

This means that the definition of 'advertisement' is very important. The Code defines an 'advertisement' in relation to a provider as 'any written, printed, electronic or oral communication ... which is directed to ... any client on request, by any such person, which is intended merely to call attention to the marketing or promotion of financial services offered by such person, and which does not purport to provide detailed information regarding any such financial services ...'¹⁸ Never mind, TL;DR.¹⁹ The definition is meant to distinguish direct marketing from advertisements aimed at the public but which do not provide detailed information to a specific client regarding a specific financial service.



Food for thought: Is this definition of direct marketing consistent with POPIA's definition of direct marketing? According to the Code, you have to be rendering a financial service (e.g., furnishing advice).²⁰ The definition in POPIA is a great deal wider. It includes communications with the indirect purpose of promoting a financial product. **Hold this thought.**

The Code creates an opt-out system from 'unwanted direct advertising.'²¹ It provides the following:

Where a provider or any person acting on its behalf uses a telephone or mobile phone call, voice or text message or other electronic communication for an advertisement, it must allow the client during that call or within a reasonable time after receiving the message, the opportunity to demand that the provider or other person does not publish any further advertisements to the client through any of these mediums.

A provider or any person acting on its behalf may not charge a client a fee or allow a service supplier to charge a client a fee for unsubscribing.²²

What you need to know: Remember that in any given scenario, the legislation that is 'more extensive' will prevail.²³ **This means that POPIA will apply in respect of electronic direct marketing.** The Code's provisions will apply to telemarketing, but only to the extent that the financial service provider is 'furnishing advice'. If the marketing in question does not meet the more restricted definition of the Code, section 11(3)(b) will give the data subject the right to object to direct marketing (POPIA's version) via telephone in any event.

This means that yes, you can still do SMS marketing for financial products, but section 69 of POPIA will apply. Therefore, you will need to comply with section 69 requirements to send direct marketing via SMS for financial products. Please see question 1.3 for the discussion of how to comply with section 69 of POPIA.

¹⁵ By GN 706 in GG 43474 of 26 June 2020, available at https://www.gov.za/sites/default/files/gcis_document/202006/43474gon706.pdf.

¹⁶ Section 14(9) of the amended General Code of Conduct for Authorised Financial Services Providers and Representatives.

¹⁷ Section 14(9) of the amended General Code of Conduct for Authorised Financial Services Providers and Representatives.

¹⁸ The definition of 'advertisement' in section 1(1) of the amended General Code of Conduct for Authorised Financial Service Providers and Representatives.

¹⁹ Too Long; Didn't Read.

²⁰ See the definition of 'financial services' in the Financial Advisory and Intermediary Services Act 37 of 2002. This leads you to the definition of 'financial service provider' which is defined as 'any person, other than a representative, who as a regular feature of the business of such person (a) furnishes advice; or (b) furnishes advice and renders any intermediary service; or (c) renders an intermediary service'. Now we should discuss the definition of 'intermediary service', but we do not want to. Another Russian nesting doll of an Act. Lawyers, urgh.

²¹ The description of 'direct advertising' is similar to 'direct marketing by means of electronic communications' in POPIA, but 'direct advertising' also includes telemarketing, which falls outside the ambit of 'electronic communication' in POPIA.

²² Section 14(9) of the amended General Code of Conduct for Authorised Financial Service Providers and Representatives.

²³ Section 3(2)(a) of POPIA.

1.3 How do we build an opt-in list and how can we go about communicating with them?

This then brings us to consent, or 'the c-word' as we call it. One of the most enduring myths about POPIA is that you can do whatever you like with personal information as long as you have consent. The number of blanket consents we see hidden in terms and conditions is nothing short of staggering. Most of these consents will be invalid. That is because POPIA defines consent as a 'voluntary, specific and informed expression of will'.²⁴ These are the elements of consent and what they mean in practice:

Voluntary

It must be a genuine choice. The data subject has to be able to say no, but still continue with the activity (e.g., to purchase a product or service or apply for employment).²⁵ The consent should also not be bundled with terms and conditions – the data subject has to have the freedom to withhold consent, but still accept the terms and conditions.²⁶ In other words, no 'fit in or f-off' consents. Data subjects must be free to withdraw consent without undue effort and without any detrimental effects such as an increase in cost, a cessation of services or a decrease in service levels.²⁷

Specific

The consent must always relate to a specific, well-articulated purpose.²⁸ A blanket consent covering all purposes for which personal information is processed will be too vague to be valid. Instead, consents must be granular.²⁹

Informed

The consent must be worded in such a way that the data subject is put in a position to make an informed decision. This means that they must have an understanding of the facts of the situation and the implications of granting or withholding consent. The European Data Protection Board is of the view that the following information must be provided for a consent to be valid:³⁰

- the identity of all of the responsible parties who will be relying on the consent
- the purpose of each processing operation for which consent is asked
- the type of personal information that will be collected and used
- that the data subject can withdraw consent; and
- whether the information will be used for automated decision-making.

POPIA does not provide that responsible parties must use plain language. However, we would argue that a consent that is not in plain language will not meet the requirement that consent must be informed. In addition, the relationship between the responsible party and the data subject may be governed by the Consumer Protection Act 68 of 2008, which provides that '[t]he producer of a notice, document or visual representation that is required, in terms of [the Consumer Protection Act] or any other law [like POPIA]' must provide the notice in plain language.³¹

Expression of will

The consent must be explicit, which means that it has to be given by means of a clear, unambiguous, affirmative act. It cannot be given by default and silence or inactivity cannot be taken as consent. To avoid ambiguity, the action of giving consent must also be distinct from other actions such as agreeing to terms and conditions.³²

²⁴ See the definition of 'consent' in section 1 of POPIA.

²⁵ European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679 10, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

²⁶ European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679 7 and 10, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

²⁷ European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679 13, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

²⁸ European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679 13, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

²⁹ European Data Protection Board Guidelines 05/2020 on Consent under Regulation 2016/679 12, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

³⁰ European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679 15, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

³¹ Section 22(1) of the CPA.

³² European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679 18, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Section 69(1) distinguishes between unsolicited direct marketing and direct marketing that is sent to a data subject that is a customer of the responsible party. Section 69(1)(a) provides that responsible parties can only send unsolicited direct marketing to data subjects if they have consented.

While the consent still has to be a voluntary, specific and informed expression of will, section 69(1) has its own additional requirements.

Enter Form 4. In the POPIA Regulations, the Information Regulator has issued a form ('Form 4') which must be followed when consent is obtained from the data subject in these circumstances.³³



Food for thought: Do responsible parties have to use the form verbatim? No. The rationale for this answer is hidden. The definition of 'form' in the POPIA Regulations provides that the forms that are attached to the POPIA Regulations must be used 'or any form which is substantially similar to that form'.³⁴ To be considered substantially similar to Form 4, it does not have to use the exact wording or layout of Form 4, but your direct marketing consent form must comply with the essential elements of Form 4.

We have broken down Form 4 into its essential elements below, which responsible parties must fulfil to have a valid consent under POPIA to send direct marketing by means of unsolicited electronic communications to data subjects:

Full name of the data subject who gives consent

Form 4 requires the 'name of data subject' in Part A and the 'full name of data subject' in Part B. We know that many responsible parties in the past have only collected the email address or the cell phone number of the data subject. Additionally, we think this is breaching POPIA's own principle of minimality regarding personal information.³⁵ In our opinion, as long as the consent recorded is linked to the data subject via an email address, cell phone number or account name that distinctly identifies the data subject, this will comply with Form 4's requirements.

The signature of the data subject

It can be signed in person or electronically.³⁶ Even though the form looks like it has to be completed as a hard copy, the definition of 'submit' in the POPIA Regulations includes electronic submissions. The signature does not have to be an advanced electronic signature.

The date and location where consent is given

As long as this data is captured by the responsibility in the back end, this is sufficient.

The identity and contact information of the responsible party (the relevant organisation's details)

This is important. To meet the POPIA requirement that consent must be a 'voluntary, specific and informed expression of will',³⁷ the data subject needs to know the exact identity of the responsible party.

The identity, contact information and signature of the person designated to act on behalf of the responsible party (usually the information officer or the deputy information officer)

This is a controversial requirement, but some privacy lawyers argue that this is a 'standard form', so as long as the responsible party has a record of an authorised person signing this consent form off, it will be sufficient. We suggest that the responsible party should keep a record of who approved the consent form used. We will keep you updated if there with further developments providing more clarity on this part of the form.

³³ Form 4 of the Regulations relating to the Protection of Personal Information, 2018 ('the POPIA Regulations') read with section 69(2)(b) of POPIA.

³⁴ Section 1 of the POPIA Regulations.

³⁵ Section 10 of POPIA.

³⁶ Section 1 of the POPIA Regulations also includes a definition of 'signature' and 'submit'. 'Signature' includes an electronic signature as defined in the Electronic Communications and Transactions Act. 'Submit' includes submit by data message, electronic communication, registered post, electronic mail, facsimile and personal delivery. This means that a consent for direct marketing may now be signed and submitted electronically.

³⁷ See the definition of 'consent' in section 1 of POPIA.

The responsible party must specify what goods or services they will be marketing to the data subject

Consent must always be 'specific' and 'informed'.³⁸ When creating Form 4, the Information Regulator indicated that in this context, this means that the responsible party must describe the goods or services in sufficient enough detail, so the specific purpose of the consent is clear.³⁹ But, how long is a piece of string? Must the responsible party list every product or service? Clearly, this would not be practical. Instead, it should be clear to the data subject what category of goods or services will be marketed to them.⁴⁰ In addition, if it is clear from the context what type of goods or services will be marketed, we do not think that the consent needs to expressly reference the type of goods. The rule of thumb is that the data subject must not be surprised to receive direct marketing about a particular good or service. For example, if a data subject consented to receive direct marketing about 'groceries', they may be surprised to receive direct marketing about life insurance from the responsible party.

The responsible party must specify the electronic communication channels they will use

For the consent to fulfil these requirements of being 'specific' and informed, the channel(s) which the responsible party will use must be specified.

In addition, instructions on how to unsubscribe must be provided to the data subject.



Food for thought: If the responsible party wants to use this direct marketing consent for cross-selling with other entities within their group or other third parties, the responsible party must get additional consents from the data subject for each of these other entities or third parties. The consent must specifically list all the parties who can send direct marketing to the data subject.⁴¹ Organisations cannot rely on vague third-party consents such as 'you consent to your personal information being shared with carefully selected third parties for direct marketing purposes!'

1.4 What if the data subject is already a customer?

If the data subject is a customer of the responsible party, the responsible party has to comply with the requirements of section 69(3) as it is then necessary to for consent using Form 4. In this section, we discuss the following requirements:

- the responsible party obtained the contact details of the data subject 'in the context of the sale of a product or service',
- the responsible party is marketing their '**own similar** products or services', AND
- the data subject was given a reasonable opportunity(s) to object.

Please remember: If a responsible party does not comply with all three of these requirements or cannot prove that they comply, section 69(3) does not apply. This means that the responsible party would have to obtain a consent that complies with Form 4. This is often referred to as 're-permissioning' or 're-consenting' an existing database. It is not something that marketers like doing, because low response rates will shrink the database substantially. Do not do it unless you absolutely have to! If you do have to, get advice on how to do it and speak to the creatives (not just the lawyers) about how to do it. We are not the first country to go through this change, and there is a lot we can learn from how other marketers dealt with it.⁴²

³⁸ Consent is defined in POPIA as a 'voluntary, specific and informed expression of will! See the definition of 'consent' in section 1 of POPIA.

³⁹ See EDPB 'Guidelines 05/2020 on consent under Regulation 2016/679' at para 57, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

⁴⁰ See Article 29 Working Party Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, page 5, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp90_en.pdf. What should those categories be? For inspiration, we look at the industry categories used by Statistics South Africa, available at http://www.statssa.gov.za/?page_id=4519

⁴¹ EDPB 'Guidelines 05/2020 on consent under Regulation 2016/679' at para 65, available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

⁴² Here is a good example of advice on how to plan for and do a re-permissioning campaign: <https://econsultancy.com/gdpr-examples-repermissioning-emails-campaigns/>. Not all of the campaigns will meet the POPIA standard, but they are good for some inspiration!

1.4.1 Contact details obtained 'in the context of the sale of a product or service'

As discussed above, the data subject must be a customer of the responsible party. This requirement confirms that the contact details must have been collected during the sales process and not after the transaction was concluded. If a responsible party only collects the contact details at a later stage, for the purpose of direct marketing, the responsible party will need to obtain consent using Form 4.

Could 'in the context of the sale of a product or service' mean that section 69(3) will apply if the contact details are obtained well before the sale of a product or service or must it have been obtained as part of the negotiations? We believe that as long as there was a transaction, it does not really matter when the contact details were first collected.



Food for thought: Must the responsible party obtain the information directly from the data subject for the requirement to be fulfilled? In the EU the requirement has been interpreted to mean that the contact details must be obtained directly from the data subject and not (for instance) from a list broker.⁴³ Be careful though! Article 13(2) of the EU Directive on Privacy and Electronic Communications⁴⁴ states that 'where a natural or legal person obtains from its customers their electronic contact details for direct marketing' while section 69(3)(a) is formulated 'if the responsible party obtained the contact details of the data subject in the context of the sale of a product or service'; POPIA does not state where the contact details must have been obtained from. Section 12 of POPIA contains a list of instances when it will be acceptable for responsible parties to collect information from sources other than the data subject. The point here is that it is permissible, even for direct marketing purposes.

1.4.2 The responsible party's 'own similar products or services'

Section 69(3) only applies to direct marketing that is sent by the same responsible party who collected the contact details and entered into the transaction with the data subject. In other words, section 69(3) cannot be used to justify direct marketing sent by (or for) another responsible party.

In addition, the products or services that the responsible party is marketing must be 'similar' to the products or services the data subject purchased. In other words, section 69(3) cannot be used as a justification to cross-sell products or services, even if the other (different) products or services are sold by the same responsible party. A consent that complies with Form 4 will have to be obtained for other products or services.



Food for thought: How similar is similar enough? The ordinary meaning of 'similar' is 'having a resemblance in appearance, character, or quantity, without being identical'.⁴⁵ For instance, if a data subject has purchased apples from the responsible party before (and this is how the responsible party obtained the data subject's contact details), under section 69(3) of POPIA it would be perfectly appropriate for the responsible party to send the data subject direct marketing about oranges. This is because these goods are in the same category (food). Life insurance or credit, on the other hand, is an entirely different type of product. If the responsible party wants to send this data subject direct marketing about life insurance or credit, the responsible party will need to get an additional consent from the data subject to do so. The line can get a whole lot blurrier when goods are 'kind of' related to each other. E.g., a travel company that markets flights can ask for consent again if they start renting out vehicles. If a data subject booked a flight from that company, does it mean that the company can rely on section 69(3) to market vehicle rentals to that customer without first asking for consent? Both fall in the category of 'transport' and are often bought together, so we believe the answer is yes.

⁴³ Information Commissioner's Office *Direct Marketing*, paragraph 133, available at <https://ico.org.uk/media/1555/direct-marketing-guidance.pdf>

⁴⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

⁴⁵ Oxford Dictionary, available at <https://www.oed.com/>

The ICO considered this question and stated:⁴⁶ 'We consider that the key question here is whether the customer would reasonably expect messages about the product or service in question. This is likely to depend on the context – including the type of business and the

category of product. For example, someone who has shopped at a supermarket might reasonably expect messages about a much wider range of goods than someone who has shopped at a specialist store for a specialist product.

Example: A customer buys groceries online from a large supermarket chain. Although they only bought bread and bananas on that occasion, they might reasonably expect emails about a wide range of products – including bread, fruit, and other groceries, but also books, DVDs, kitchen equipment and other everyday goods commonly sold in supermarkets. However, they are unlikely to expect emails about banking or insurance products sold under the supermarket brand. These products are not bought and sold in a similar context.'

Responsible parties should focus on managing the expectations of data subjects about what type of marketing they can expect to receive at the point of sale; data subjects who are not surprised about what they are going to receive will (probably) not complain.

1.4.3 Reasonable opportunity(s) to object

Section 69(3) will only apply if the data subject was given a reasonable opportunity to object to the use of his or her 'electronic details' at the time the information was collected; and on the occasion of each communication with the data subject for the purpose of marketing.

There are two aspects that are important here:

- the form of the unsubscribe; and
- when it must be communicated to the data subject.

We discuss the form of the unsubscribe below. As for the timing, in order to rely on section 69(3), the responsible party will have to show that the data subject was informed and given an opportunity to object at collection and again every time they were contacted.

Tricky area: What if the personal information was not collected from the data subject directly? It is not a requirement that the contact details are obtained from the data subject directly for section 69(3) to apply. In cases where the information was collected from another source, we apply section 18(2)(b) which provides that where information was not collected from the data subject, notification can take place 'as soon as reasonably practicable after it has been collected'. However, if notification of the right to unsubscribe did not take place at all (for whatever reason),⁴⁷ the responsible

party cannot rely on section 69(3) and would have to ask for consent and comply with Form 4.

What this means is that the responsible party has to prove that this information was given to data subjects, even where collection took place decades ago!

1.4.4 Requirements for a valid unsubscribe

Data subjects have the right to 'unsubscribe' from direct marketing. It is referred to as the right to object, but most of us know this as unsubscribing.

Please note: This not only applies to electronic direct marketing, but also in respect of non-electronic forms of marketing.

Once a data subject has unsubscribed, the responsible party must stop sending direct marketing to that data subject. Internationally under the EU GDPR, many companies have been fined large sums by regulators for failing to process their unsubscribes properly. For example, in March 2020 a Romanian company was fined approximately EUR3000 for sending a commercial message to just one customer who had already unsubscribed.⁴⁸ Additionally, in October 2019, a Greek telecommunications company was fined EUR200,000 for contacting a large number of customers via telemarketing when all these customers had specifically opted out of receiving telemarketing from them. The unsubscribes had not been processed properly

⁴⁶ Information Commissioner's Office *Direct Marketing*, from paragraph 136, available at <https://ico.org.uk/media/1555/direct-marketing-guidance.pdf>

⁴⁷ Including acceptable reasons not to notify in terms of section 18(4).

⁴⁸ OneTrust DataGuidance 'Romania: ANSPDCP fines Dante International €3,000 for GDPR violation' available at <https://www.dataguidance.com/news/romania-anspdcf-fines-dante-international-%E2%82%AC3000-gdpr-violation>

due to technical issues.⁴⁹ These examples demonstrate how important it is to manage direct marketing unsubscribes properly for all forms of direct marketing, and the negative repercussions organisations can face if they do not.

Please note: In addition to a potential fine by the Information Regulator, a complaint for failing to honour an unsubscribe has other consequences. The cost and inconvenience of being investigated by the Information Regulator will be significant and once the Information Regulator starts investigating an organisation, there is no telling where the investigation could lead.

There are no general requirements in POPIA for the form the unsubscribe must take. However, when unsubscribes are being considered for purposes of section 69(3)(c), the following requirements are listed:

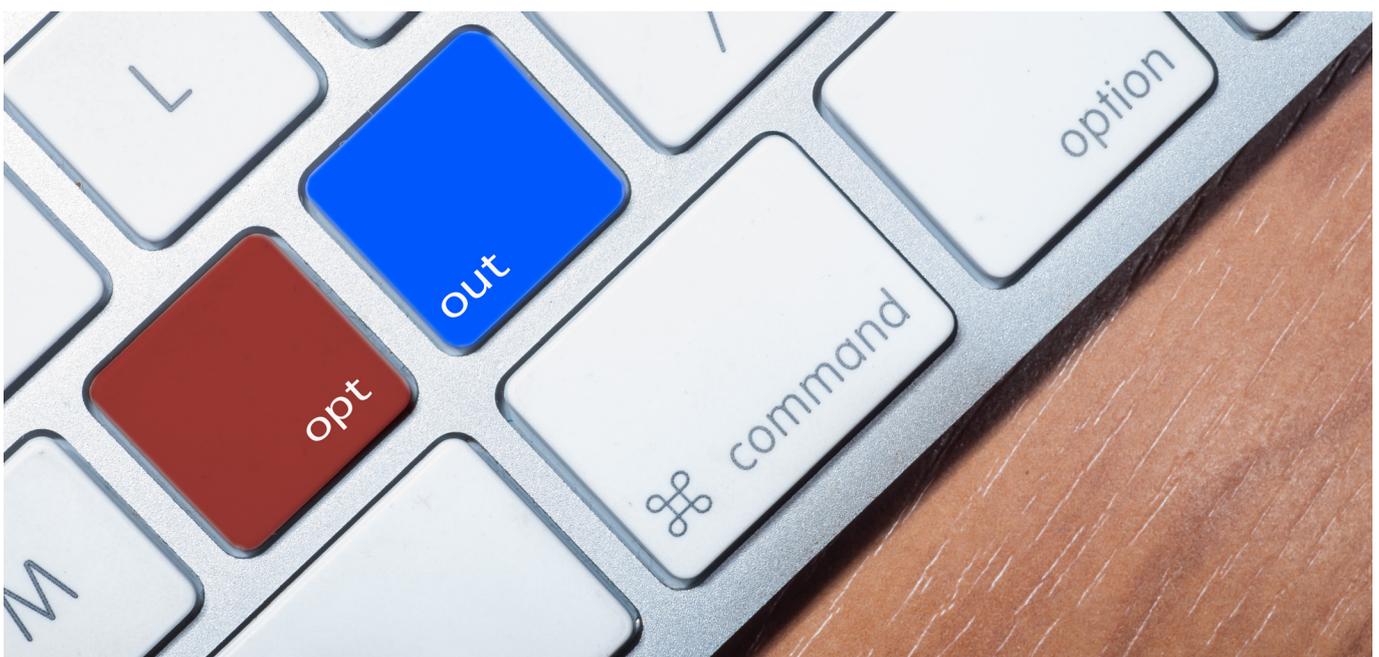
- It must be free of charge.
- The opportunity to unsubscribe must be 'free of unnecessary formality!'

Please note: We believe that these requirements should be viewed as 'best practice' for all unsubscribes, not just when compliance with section 69(3) is being considered. In other words, we believe that these requirements should be applied when considering compliance with section 11(3)(b) too, even though the requirements are not mentioned there. In any event, if the direct marketing is being sent to a consumer as defined in the CPA, section 11 provides that a responsible party must 'implement appropriate procedures to facilitate the receipt of [unsubscribes] and must not charge the consumer a fee for unsubscribing.'⁵⁰

The requirement that the unsubscribe must be free of charge is quite clear, albeit not always simple to execute. However, defining what would constitute 'unnecessary formality' is harder to quantify.

Here are the guidelines provided by the ICO:⁵¹

- It must be simple to opt out.
- When first collecting the data subject's details it must be part of the same process (e.g. the form should contain a prominent opt-out box or staff should offer it when information is being collected 'in person').
- In subsequent communication, the data subject should be able to unsubscribe by replying to the message or by clicking on an unsubscribe link.
- If the marketing is taking place via SMS, the data subject should be able to unsubscribe by sending a stop message to a short code.



⁴⁹ OneTrust DataGuidance 'Greece: HDPAs fines telecom service provider for GDPR violations' available at <https://www.dataguidance.com/news/greece-hdpa-fines-telecom-service-provider-gdpr-violations>

⁵⁰ Sections 11(4)(a) and 11(5) of the CPA.

⁵¹ Information Commissioner's Office *Direct Marketing*, paragraph 138, available at <https://ico.org.uk/media/1555/direct-marketing-guidance.pdf>

1.5 Are members allowed to keep a database purchased for direct marketing purposes prior to 1 July? If yes, how are they allowed to use a database like that after 1 July? Will we be allowed to purchase third party data to utilize when doing so?

For our view on the buying and selling of third party databases – and how to do this in a POPIA-compliant way – please see the **'10 Guiding Principles of Ethical Lead Generation'**

Concerning whether you can keep a database purchased for direct marketing purposes prior to 1 July 2021, this is not a clear-cut 'yes/no' answer. It is usually very dependent on the individual context of each responsible party. Or usual motto is 'don't throw the database out with the bathwater' unless you have done a thorough investigation first.

Suppose the data subject is a customer of the responsible party. In that case, the responsible party has to comply with section 69(3) requirements to avoid asking for consent to send direct marketing using Form 4. The responsible party must meet the following requirements:

- the responsible party obtained the contact details of the data subject 'in the context of the sale of a product or service,'
- the responsible party is marketing their 'own similar products or services,' AND

- the data subject was given a reasonable opportunity(s) to object.

If a responsible party does not comply with all three of these requirements or cannot prove that they comply, section 69(3) does not apply. This means that the responsible party would have to obtain a consent that complies with Form 4. This is often referred to as 're-permissioning' or 're-consenting' an existing database. It is not something that marketers like doing because low response rates will shrink the database substantially. Do not do it unless you absolutely have to! If you do have to, get advice on how to do it and speak to the creatives (not just the lawyers)⁵² about doing it. We are not the first country to go through this change, and there is a lot we can learn from how other marketers dealt with it.⁵³

To streamline an organisation's direct marketing efforts to be POPIA compliant, we advise that organisations should go about a spring cleaning and rebuilding exercise of their direct marketing database.

As best practice for achieving POPIA compliance, an organisation should be able to answer the following questions about all the data subjects in their direct marketing database:

- Where the organisation got each data subject's personal information, i.e., did the organisation get it straight from the data subject, did the organisation get it from a public record or social media, did the organisation get it from a different entity in their same corporate group, did the organisation get it from a credit bureau or did the organisation buy it from a lead generation company or data broker?
- Whether each data subject has consented to receive direct marketing from the organisation, if the answer is yes, then the organisation needs to determine which specific brand/product the data subject has consented to receive direct marketing about and what channel of communication the data subject chose to receive direct marketing by. If the answer is no, the organisation needs to check if that data subject has requested to unsubscribe from direct marketing and if that unsubscribe has been processed properly.
- If each data subject is allowed to unsubscribe on each different direct marketing occasion.
- If the organisation has shared each data subject's personal information with any third party and for what reason.

⁵² As Dr McCoy from Star Trek would say: 'Damn it Jim, I'm a lawyer not a marketer!'

⁵³ Here is a good example of advice on how to plan for and do a re-permissioning campaign: <https://econsultancy.com/gdpr-examples-repermissioning-emails-campaigns/>. Not all of the campaigns will meet the POPIA standard, but they are good for some inspiration!

Once the organisation has established the answers to these questions concerning their direct marketing database, we have made this handy table to assist with making the right spring-cleaning decision based on the above exercise results.

Where you got the lead/customer's personal information from	POPIA implications
The organisation has already sold something to this customer and is now marketing similar products also provided by the organisation.	If the organisation told the data subject that they would get direct marketing and always allowed them to unsubscribe, the organisation can carry on marketing to them.
The organisation has no idea where the data subject's personal information came from.	If the organisation can't prove where the data subject's personal information came from and the circumstances under which it was obtained, POPIA requires that the organisation notify the data subject that the organisation has their information and ask for the data subject's consent to continue marketing to them.
The organisation has already sold something to this data subject, but now is cross-selling a completely different product also provided by the organisation.	The organisation will need the data subject's consent before the organisation markets to the data subject.
The organisation got the data subject's personal information from another entity in the same group of companies.	The organisation will need the data subject's consent to market to them. The organisation may even require the data subject's consent before the data subject's personal information is shared between entities in the group.
The organisation got the data subject's personal information from a credit bureau, lead generation company or another entity unrelated to the organisation.	<p>The organisation will need the data subject's consent to market to them. The entity sharing the data subject's information with the organisation may require the data subject's consent before sharing.</p> <p>If the entity sharing the data subject's personal information is asking for consent for direct marketing on the organisation's behalf (a third party consent), the organisation must be mentioned by name for that consent to be valid.</p>
The organisation scraped the data subject's personal information from the internet or a public record.	The organisation will need the data subject's consent to market to them. The organisation may even need data subject's consent just to have their personal information. Or the organisation will need to meet one of the other requirements for legally collecting a data subject's personal information from a third party in terms of section 12.



1.6 What does POPIA say about collecting a data subject's personal information from a third party source and notifying the data subject about this collection?

Section 12 of POPIA deals with the collection of personal information. The default rule in section 12(1) of POPIA is that responsible parties must always collect personal information directly from the data subject. There are exceptions to this rule, however. These are outlined in section 12(2) of POPIA. These include:

- Personal information in or derived from a public record;
- Personal information which the data subject deliberately made public;
- The data subject consent to the collection of their personal information from third parties;
- The responsible party can demonstrate that collecting the personal information from another source does not prejudice a legitimate interest of the data subject;
- Collection from third-party sources is required for law and order;
- Collection from a third party is necessary to maintain the legitimate interests of the responsible party or a third party;
- Collection directly from the data subject prejudices a lawful purpose of the collection; and
- The responsible party does not have to collect the personal information from the data subject

if this is not 'reasonably practicable in the circumstances of the particular case'

It is also important to note that in most circumstances, if you are collecting a data subject's personal information from a third party source (whatever the legal justification) – you are required to notify the data subject about this collection in terms of section 18.

In cases where the personal information is collected from another source the data subject must preferably be notified before collection occurs⁵⁴ or, if that is not possible, 'as soon as reasonably practicable after it has been collected.'⁵⁵ It is a pity that POPIA did not provide more specific guidelines in this regard. The EU GDPR provides that the notifications must be made:⁵⁶

- within a reasonable time after collection, 'but at the latest within one month, having regard to the specific circumstances in which the personal data are processed';
- 'at the latest at the time of the first communication' with the data subject (if the personal data will be used to communicate with the data subject); or
- before the personal information is shared with any 'recipient.'⁵⁷



Food for thought: Even though POPIA is silent on what would qualify as 'as soon as reasonably practicable', the standard set by the EU GDPR is a useful indication of 'best practice'. Responsible parties should carefully document their decision-making process when they determine when data subjects will be notified and be ready to defend their decision about when to notify.



⁵⁴ Section 18 of POPIA.

⁵⁵ Section 18(2)(b) of POPIA.

⁵⁶ Article 14(3).

⁵⁷ A 'recipient' is defined as 'a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.' Article 4(9).