

# POPIA Explained – Part 9

By Lize de la Harpe, legal adviser

In the last edition we recapped on the eight conditions for the lawful processing of personal information and discussed the final condition, namely Data subject participation.

In this edition we will discuss the concept of consent and see exactly when it is needed and what the requirements are for valid consent.

## Grounds for lawful processing

As explained previously in Part 3 (Conditions for lawful processing), responsible parties must always be able to base their processing on one of the grounds as provided in section 11(1), otherwise they will not be allowed to process the personal information.

Section 11(1) forms part of Condition 2 (being Processing Limitation) and deals with the consent required for processing, the justification of processing and the objection thereto by the data subject.

Section 11(1) states that personal information may only be processed IF:

- a. the data subject consented; OR
  - processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party (*\*for example, where a product provider processes information contained in an application form for an investment contract*); OR
  - processing complies with an obligation imposed by law on the responsible party (*\*for example, where personal information is provided to SARS in terms of the Income Tax Act or to comply with a court order*); OR
  - processing protects a legitimate interest of the data subject (*\*for example where a retirement fund is required to trace a “dependant” as defined in the Pension Funds Act and discloses the dependant’s details to a tracing agent*); OR
  - processing is necessary for the proper performance of a public law duty by a public body (*\*for example, where the police request information from a responsible party regarding one of its clients in connection with an investigation*)

); OR

- processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied (*\*for example, where processing is necessary for the investigation of fraud or other misconduct*).

To summarise: responsible parties must always be able to base their processing of personal information on at least ONE of the grounds set out above, otherwise they will not be allowed to process the information. Consent is one of the grounds for lawful processing.

Do you always need the data subject's consent?

No! Despite the common misconception that the data subject's consent is *always* required, you can clearly see from the wording of section 11(1) quoted above that consent is merely ONE of the grounds for lawful processing (*hence the word "OR" in between sub-sections (a) to (f)!*).

To put it differently: if *none of the other exceptions* as listed in (b) to (f) apply, you will need the data subjects' consent in order to process the personal information.

Several clauses in POPIA contain the requirement that consent must be obtained as an alternative to other justifications. Examples include:

- Section 12 (collection directly from data subjects) which states personal information must be collected directly from the data subject except if (*inter alia*) the data subject consented to the collection from another source;
- Section 14 (retention and restriction of records) which states records may not be kept for longer than is necessary for achieving the purpose for which it was collected *except where* (*inter alia*) the data subject has consented to the retention of the record;
- Section 15 (further processing to be compatible with the purpose) which states that further processing is not incompatible with the purpose of collection if (*inter alia*) the data subject consented to the further processing;
- Section 27 (general authorisation concerning special personal information) which states that the prohibition on processing special personal information does not apply if (*inter alia*) the processing is carried out with the consent of a data subject, or processing is for historical, statistical or research purposes to the extent that it appears to be impossible or would involve a disproportionate effort to ask for consent;

- Section 72 (transfers of personal information outside the Republic) which states that a responsible party in the Republic may not transfer personal information about a data subject to a third party that is in a foreign country *unless (inter alia)* the data subject consents to the transfer.

Again – each of the examples listed above refers to consent as ONE of the exceptions to the particular rule.

There are however certain instances where the data subject's consent will be required, for example in certain cases of cross selling (as discussed in Part 5 - Further Processing Limitation) and for purposes of direct marketing (\*PS: we will discuss direct marketing in the next edition).

What constitutes valid consent?

POPIA sets very specific requirements for consent to be valid. To understand these requirements, we have to carefully look at the definition of "consent" as set out in section 1 of the act.

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

Now, let's break the definition down into smaller bits and look at each "piece" in more detail in order to determine the specific requirements that "consent" must meet in order to be valid:

1. it must be an expression of will;
2. given voluntary;
3. be specific; and
4. be informed.

#### 1. An expression of will

The act does not prescribe written consent (\*the definition of consent refers to "....any....expression of will...") – which means that *in principle* there is no limit as to the form the consent can take. For example, consent can take the form of signatures, oral statements to express agreement or a behaviour from which consent can be reasonably concluded.

However, for consent to be valid, it must be an "expression of will... .. in terms of which permission is given..." (\*PS: one should be cautious when relying on implied consent, i.e.: the absence of any behaviour/passive behaviour – the words "expression of will" seem to imply a need for action, so a simple inaction might not be enough to constitute consent!)

Remember: section 11(2)(a) clearly states that the responsible party bears the burden of proof that the data subject's consent was obtained. It is therefore advisable to obtain written consent as proof (\*PS: *even when there is proof of consent, the data subject can still object on the basis that the said consent was not "voluntary" and/or "informed"*).

## 2. Given voluntary

The data subject must be able to freely exercise a real choice ("...voluntary... expression of will..."), which means there must be no risk of deception, intimidation or significant negative consequences if he/she does not consent. Any consent given under duress or fear of negative consequences would not be a "voluntary ...expression of will".

## 3. Be specific

Consent must be specific. In other words, a *blanket authorisation* to process personal information which does not specify the exact purpose of processing will NOT be valid.

To be specific, consent should refer clearly and precisely to the scope and the consequences of the data processing - which data will be processed and for which purpose (\*PS: *it cannot apply to an open-ended set of processing activities*).

## 4. Be informed

The requirement that consent must be specific (discussed above) is inherently linked to the requirement that consent must be informed.

To be valid, consent must be given on an informed basis. All the necessary information must be given when the consent is requested which points out to the data subject, in particular, the nature of the information processed, the purposes of the processing, the recipients of transfers (where applicable) and the rights of the data subject.

Although the *timing* for obtaining consent is not addressed outright in the act, it is clearly implied from the wording of the relevant sections that (*as a general rule*) consent must be obtained before the processing starts.

## Opt-in or opt-out?

The way in which consent is obtained may vary, depending on the circumstances and the type of information:

- Opt-in consent refers to instances where the data subject actively agrees to the purpose, i.e.: by saying "yes";
- Opt-out consent refers to instances where, unless the data subject actively opts out of the

stated purpose, i.e.: by saying “no”, consent may be assumed.

Opt-out consent is generally sufficient, but opt-in consent would be required for purposes of processing special personal information (discussed in Part 2 – Types of personal information) and direct marketing (\*PS: we will discuss direct marketing in the next edition).

## Withdrawal of consent

Section 11(2)(b) states that a data subject (or competent person) may withdraw his/her consent at any time, *provided that* the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of sections 11(1)(b) to 11(1)(f) (summarised above) will not be affected.

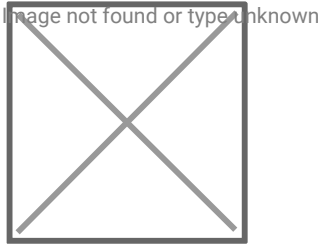
Responsible parties must provide a convenient way for data subjects to withdraw consent (\*and manage such withdrawals!) and must also explain the consequences of the withdrawal of consent to the data subject (\*for example, if a client refuses their consent to a credit check, the insurer may not be able to offer the client products for which credit worthiness is relevant).

## Conclusion

We can all agree that consent is a vital part of the fundamental right to protect personal information. However, and as you can see from the above, consent is not the only legal ground for the lawful processing of personal information.

Consent, when required, must meet the above requirements in order to be valid. Any forms used to obtain consent should clearly identify the purposes for the collection, use and disclosure of the data subject’s personal information. It is also important to ensure that employees involved in obtaining the client consents are adequately trained to explain the nature and scope of the consent sought.

Responsible parties relying on consent should also consider ways to keep record of consents which have been obtained (\*i.e.: creating and maintaining records showing that the consent was indeed given). Lastly, responsible parties must keep in mind that obtaining consent does not amount to an exemption from the *other conditions set out in the act!*



## Lize de la Harpe

Lize de la Harpe obtained an LLB degree in 2005 from the University of Stellenbosch, whereafter she completed her articles and was admitted as an attorney in the Cape High Court. During 2008 she completed a Postgraduate Diploma in Financial Planning (CFP) from the University of the Free State. Lize joined Glacier in June 2012 as the legal adviser and principal officer. Prior to joining Glacier, she worked as legal counsel in the investment cluster at Momentum for four years.

**This document is intended for use by clients, alongside their financial intermediaries.** The information in this document is provided for information purposes only and should not be construed as the rendering of advice to clients. Although we have taken reasonable steps to ensure the accuracy of the information, neither Sanlam nor any of its subsidiaries accept any liability whatsoever for any direct, indirect or consequential loss arising from the use of, or reliance in any manner on the information provided in this document. For professional advice, please speak to your financial intermediary.

Glacier Financial Solutions (Pty) Ltd.

A member of the Sanlam Group

Private Bag X5 | Tyger Valley 7536 | Email [client.services@glacier.co.za](mailto:client.services@glacier.co.za) | Tel +27 21 917 9002 / 0860 452 364 | Fax +27 21 947 9210 | Web [www.glacier.co.za](http://www.glacier.co.za) | Reg No 1999/025360/07

Licensed Financial Services Provider | Glacier Financial Solutions (Pty) Ltd. is also a Licensed Discretionary Financial Services Provider FSP 770, trading as Glacier Invest | Sanlam Multi-Manager International (Pty) Ltd. | A member of the Sanlam Group

Private Bag X8 | Tyger Valley 7536 | Tel +27 21 950 2600 | Fax +27 21 950 2126 | Web [www.smmi.com](http://www.smmi.com) \*|\*Reg No 2002/030939/07

Licensed Discretionary Financial Services Provider, acting as Juristic Representative under the Glacier Financial Solutions FSP 770

Glacier International is a division of Sanlam Life Insurance Limited

Sanlam Life Insurance Ltd. | Email [life@sanlam.co.za](mailto:life@sanlam.co.za) | Tel + 27 21 916 5000 / 0860 726 526 | Fax +27 21 947 9440

Reg No 1998/021121/06 | Licensed Financial Services Provider