U.S. based callers: 1-888-376-1079
Callers from outside U.S.: +1-617-398-7067
www.verasafe.com

POPIA Privacy Policy Checklist

Introduction

While POPIA does not explicitly require that organizations maintain a privacy policy, Section 18 of POPIA states that a responsible party must take reasonably practicable steps to ensure that a data subject is aware of how an organization will process their personal information.

Publishing a privacy policy on your website is the easiest, most effective way to comply with Section 18 of POPIA.

VeraSafe created this checklist to help you create or update your organization's privacy policy in accordance with the requirements set out in POPIA.

Required Disclosures

The following twelve disclosures are required by POPIA:

1. Your organization's full name and address

The data subject whose personal information is being collected should be informed of your organization's full legal name and address.

Section 18(1)(b)

2. The nature or categories of personal information your organization collects and/or processes

Your privacy policy should outline the types of personal information that you collect and process. POPIA defines personal information as any *"information relating to an identifiable, living, natural person and where applicable, an identifiable, existing juristic person"* (for example, name, email address, physical address, bank account number, national identification number, and more).

Section 18(1)(a), read with Section 18(1)(h)(ii)

3. If personal information is not collected from the data subject, the source from which it is collected

You may collect all or some of the information from a third party (for example, a government database). In this case, you should indicate the source(s) or category of source(s) from which you obtain the personal information.

Section 18(1)(a)

4. The purpose for which your organization collects and/or processes personal information

You must state how the personal information you collect or process will be used. We recommend that you identify each purpose for which you process the different categories of personal information.

Section 13(2), read with Section 18(1)(c)

5. An indication of whether or not the supply of the personal information is voluntary or mandatory

You need to indicate to the data subject whether it is mandatory or voluntary to disclose all or certain categories of the personal information to you.

For example, to facilitate an e-commerce transaction, it is mandatory for a data subject to provide their residential address to have goods delivered.

Section 18(1)(d)

6. The consequences if the data subject does not provide the requested personal information

You must inform the data subject of the consequences of failing to provide you with the requested information.

For example, to fulfil an e-commerce order, you need the data subject's residential address. Your privacy policy should indicate that the data subject cannot use the e-commerce platform if they fail to provide their residential address.

Section 18(1)(e)

7. List any particular law authorizing or requiring the collection of personal information

In some cases, you may be under a legal obligation to collect a data subject's personal information (for example, to comply with tax or employment law requirements). If this is the case, you should list the relevant law authorizing or requiring the collection of personal information.

Section 18(1)(f)

8. Disclose if your organization intends to transfer the personal information outside of South Africa

You should indicate whether the personal information will be transferred to a third country or international organization outside of South Africa. You should also indicate the level of protection afforded to the personal information by the third country or international organization to which the information is being transferred.

Section 18(1)(g)

9. The recipient or category of recipients of the personal information

A "recipient" is a third party to which your organization may disclose the personal information (including your own affiliates). Your privacy policy must indicate the category or identity of the third-party recipients.

Section 18(1)(h)(i)

10. Existence of the data subject's right to access and right to rectify the personal information collected

Your privacy policy must inform data subjects about their rights concerning the information you process about them. This includes the right to access one's personal information and to rectify one's personal information.

Section 18(1)(h)(iii)

11. Existence of the right to object to the processing of personal information

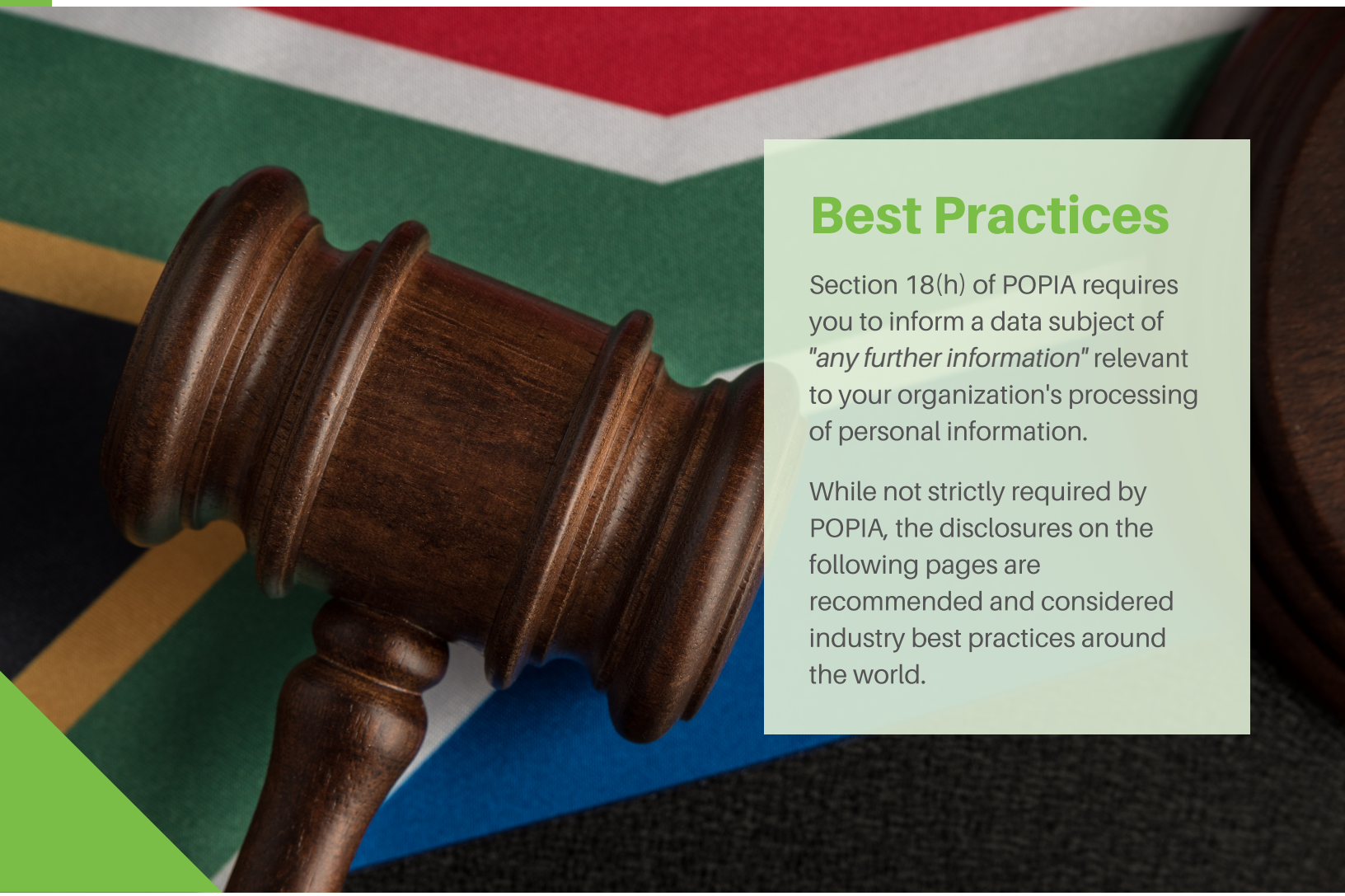
If you process personal information based on certain grounds for processing as outlined in Section 11(1)(d) to (f) of POPIA, you need to inform a data subject of their right to object to such processing.

Section 18(1)(h)(iv), read with Section 11(3)

12. The right to lodge a complaint to the Information Regulator

You must inform a data subject that they have the right to lodge a complaint to the Information Regulator. You must also provide a data subject with the relevant contact details of the Information Regulator to which the data subject can direct their complaint.

Section 18(1)(h)(v)



Best Practices

Section 18(h) of POPIA requires you to inform a data subject of *"any further information"* relevant to your organization's processing of personal information.

While not strictly required by POPIA, the disclosures on the following pages are recommended and considered industry best practices around the world.

Optional Disclosures

VeraSafe strongly recommends you also include these seven disclosures:

1. Existence of the right to withdraw consent to the processing of personal information

If you process personal information of a data subject based on consent, you should inform them of their right to withdraw consent.

2. The basis on which you collect personal information

POPIA requires that you have a lawful basis on which you process personal information. For example, the performance of a contract between you and the data subject, the legitimate interests of your organization's business, or to comply with a legal obligation.

3. Data retention policy

In line with the POPIA Condition of Openness, your privacy policy should specify how long you will store the personal information or, if not possible, the criteria used to determine that retention period. POPIA requires that personal information only be kept for as long as necessary to achieve the purpose for which it was collected.

4. Description of your security measures

Your privacy policy should provide data subjects with some general information on how you will keep their personal information secure.

5. Contact details of your Information Officer

You should include your Information Officer's name and contact details to whom a data subject can direct any questions or complaints.

6. Changes to the terms of the privacy policy

State how your organization will communicate any future changes to the privacy policy to the data subject.

7. Effective date

You should state the effective date of your privacy policy and update it each time the policy is updated.

ABOUT VERASAFE

VeraSafe offers a complete solution to help your organization comply with South Africa's most extensive law on the protection of personal information. Our specialist privacy professionals and IT security experts are uniquely placed to provide a holistic approach to compliance.

Visit our POPIA Compliance page for more information about the key elements of VeraSafe's POPIA Compliance Program.

U.S. based callers: 1-888-376-1079
Callers from outside U.S.: +1-617-398-7067
www.verasafe.com

DISCLAIMER

The information contained in this checklist does not constitute legal advice, and any organization using this checklist may not rely on it as such. Like most privacy laws, POPIA is complex and open to interpretation. It is strongly recommended that organizations seek professional legal advice on how to comply with POPIA, including the drafting of privacy policies.