OpenUp Privacy olicy

Dear Policy Reader

This policy is a useful outline to how we approach privacy protection at OpenUp, and some other information we feel it is good for the public to know. We think this applies to you if you use our websites, or engage with us more generally (for instance, as a client or beneficiary).

Please note, we understand this document is text heavy. We have tried to make it as user-friendly as possible, and are constantly working on how to make privacy (and access to information) rights easy to action for people, and easy to understand.

We will post amendments from time to time to action that commitment!

All the best,

OpenUp

Our POPIA Cheatsheet

The Protection of Personal Information Act (POPIA) is intended to protect a person's right to privacy *in terms of* your personal information and data. Personal information is not private *per se*, and POPIA doesn't say you cannot process it in general, but rather outlines how you need to process it (if you do) to stay within the bounds of the law. There is an online version of the Act available here. Here is also a cheat sheet on how to read POPIA itself:

- Chapter 3 sets out the main conditions for lawful Processing of Personal Information.
- There may be specific internal limitations within different sections.
- Chapter 3 provides for general rules applicable to the Processing of Personal Information in Part A (sections 8 to 25 of POPIA).
- There are also special conditions applicable to the Processing of Special Personal Information (in Part B: sections 26 to 33 of POPIA) and the Personal Information concerning a Child / children (in Part C: sections 34 and 35 of POPIA). In both instances, the additional specific obligations in Part B are applicable.

- But there are general exemptions from the conditions for Processing (these are contained in sections 36 to 38):
    - If the Regulator exempts you, which can be done:
        - if the public interest in the Processing outweighs, to a substantial degree, any interference with the privacy of the Data Subject that could result from such processing; and
        - the Processing involves a clear benefit to the Data Subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the Data Subject or third party that could result from such Processing; and
        - If Processing is undertaken for the purpose of discharging a defined function (essentially a function performed by a Public Body or a fraud prevention function).

Definitions that matter

Personal Information includes:

- certain information that we collect automatically when you visit our website (but you can read our cookie policy her:https://openup.org.za/cookie-policy);
- certain information collected on submission in relation tous engaging in contractual relationships of different types;
- public domain personal information (POPIA treats this information quite differently); and
- optional information that you provide to us voluntarily (see below); but excludes:
    - information that has been made anonymous so that it does not identify a specific person;
    - permanently de-identified information that does not relate or cannot be traced back to you specifically; and
    - non-personal statistical information collected and compiled by us.

Special Personal Information

This is information relating to religion, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or information relating to the criminal behaviour of a data subject. Depending on the goods or services that you require, we may also collect sensitive personal information (although that is *rarely* collected).

Our Personal Privacy Mantra

There is a presumption at OpenUp that Personal Information will only be collected by staff when absolutely necessary (in line with the principles of **minimality** and limiting collection of data to instances where there is a specific purpose for those data), and that there will be a preference for collecting, processing and preserving de-Identified data, to which POPIA will not apply.

Our Information Officer

Gabriella Razzano is the Information Officer. She can be contacted through the email infoofficer@openup.org.za. The Information Officer's role is generally to:

- Develop, implement, monitor and maintain a compliance network;
- Conduct a Personal Information impact assessment in order to ensure that adequate measures exist to ensure compliance with POPIA;
- Develop, monitor, and maintain a POPIA manual and make it available to everyone at OpenUp as required of her by sections 14 and 15 of the Promotion of Access to Information Act (**PAIA**));
- Ensure that internal measures are developed together with adequate systems to process requests for, or access to, information; and
- Conduct (or oversee the conducting of) internal awareness sessions regarding the provisions of POPIA.

Her role is to help everyone at OpenUp stay POPIA-compliant.

Why do we have your personal information?

We generally collect and process your personal information for various purposes (though each collection has its own purpose), including:

- **Research purposes** - we may have requested or gathered your information in the effort to conduct user or academic research as part of our non-profit activities that seek to forward the interests and rights of people in relation to data, technology and innovation;
- **Open data purposes** - as part of our service to the country at large, we make open data more accessible to the public - this sometimes includes personal information);
- **Goods or services purposes** – such as collecting orders or requests for and providing our goods or services (although because we are not a commercial company, this is not very common and will generally be facilitated by specific agreements);
- **Marketing purpose**s – such as pursuing lawful related marketing activities (our main channel for this is our quarterly newsletter, and we comply with POPIA in relation to its management);
- **Business purposes** – such as internal audit, accounting, business planning, and joint ventures, disposals of business, or other proposed and actual transactions; and
- **Legal purposes** – such as handling claims, complying with regulations, completing contracts or pursuing good governance.

It is very important to note that, frequently, OpenUp is collecting information *not as the responsible party* but as the **operator.** The operator is a third party to whom the processing of personal Information has been outsourced. Despite the processing being outsourced to an operator, the organisation still remains responsible for the operator's actions in terms of POPIA (for instance, maintaining security).

When we are the responsible party, OpenUp must ensure that proper agreements are in place to ensure that operators meet the requirements of POPIA. This is a person who processes personal information for OpenUp in terms of a contract or mandate, but is not under the authority of OpenUp, e.g. employees of the courier, auditors, website hosts, marketing forms, etc.

What we do with personal information

When we are the **responsible party**, and we have your personal data, we process it on the following lawful bases:

- Because you gave us your consent to do so. You are able to remove your consent at any time if you have given it to us. You can do this by contacting the Information Officer (see below "How to action your rights");
- Because we have a contractual obligation to do so (for instance in terms of a processing agreement with an operator);
- Because we have a legal obligation to do so (for instance certain employee and tax records); or
- Because we have a vital or legitimate interest in doing so.

We do not participate in any commercial exchanges of personal information in any context.

So, if we are processing your personal information personal data we commit to do so:

- lawfully, fairly and transparently;
- only for a specific purpose that is explicit and legitimate;
- only as necessary for that purpose;
- accurately, and keeping it up to date;
- for no longer than necessary to achieve the purpose; and
- Securely (read more about how we put those principles into practice in "How we action privacy".

Your rights

As a data subject, you have the following (and some more) rights under the POPIA:

- Be notified that your personal information is being collected (see further though section 18);
- Be notified of your personal information has been accessed by an unauthorised person (in other words, to be notified if we find out their has been a data breach which includes your personal data);
- To the correction, destruction or deletion of your personal information if the personal information is inaccurate; irrelevant; excessive; out of date; incomplete; obtained unlawfully; or that it is no longer authorised to retain in terms of **section 14**.

- To object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of **section 11(3)(a)**;
- to object to the processing of his, her or its personal information at any time for purposes of direct marketing (we try and facilitate this through our newsletter forms);
- to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject.

The Information Regulator and other resources

The Information Regulator's site is here. The Information Regulator is the authority put in place to oversee and enforce both POPIA, and the Promotion of Access to Information Act. If you wish to file a complaint in terms of either law, you can do so with the information on their website (which also provides the different forms you might need).

Their website has a lot of useful resources on POPIA and privacy in South Africa. Michalsons is a private law firm that also provides a lot of resources on POPIA on their website here, though largely for organisations looking to comply with POPIA rather than for the data subject.

How to action your rights

We don't believe in complicating things.

If you want to find out if we hold any personal information, email us through the Information Officer's contact details above, providing us with *sufficient personal details* to enable us to search our records.

If you want us to correct or delete your personal information, you'll need to provide us with that personal information in a manner sufficient for us to source it, and also explain in your email how it is either: **Inaccurate; Irrelevant; Excessive; Out of date; Incomplete; Obtained unlawfully**; or that it is **no longer authorised to retain** in terms of **section 14**. It is important to note that maintaining data integrity means we cannot readily delete or alter personal information, unless any of those grounds can be established.

If you have any other query or complaint about how we process *personal* data, or any other kind of POPIA-specific query, please contact us providing the details of that complaint *after consulting the FAQs below*.

Please note further - though there is no right to de-indexing in terms of the law, OpenUp will accept individual appeals to de-index (if reasonably technically possible) where the data subject can demonstrate that there is a *reasonable* and *demonstrable* belief that the existing disclosure of their personal data would lead to an imminent and serious personal safety risk, or another form of serious and irreversible personal risk that arises from the nature of the personal information, and the details of the case itself. This will be determined while balancing against the fact that it will have already been

established that this Personal Information is lawfully displayed (or else **section 14** would apply), as well as against the broader public interest in the information being easily searchable. The data subject should note there is no right to have our decision on such a matter reviewed by any existing entity in law.

How we action privacy

We have an internal POPIA policy which outlines how POPIA works in our organisation. Staff are inducted with the policy, and we conduct regular training.

We take the security of personal information very seriously and always do our best to comply with applicable data protection laws, but also industry best standards. Our Chief Technology Officer helps lead our data security measures, and we have a data breach policy in place. We use secure servers, both local and international, with advanced security measures to prevent interference or access from outside intruders. We authorise access to personal information only for those employees who require it to fulfil their job responsibilities. We implement disaster recovery procedures where appropriate.

We will try to keep the personal information we collect as accurate, complete and up to date as is necessary for the purposes defined in this policy. From time to time we may request you to update your personal information, accordingly.

We will only retain your personal information for as long as it is necessary to fulfil the purposes explicitly set out in this policy, unless:

- retention of the record is required or authorised by law; or
- you have consented to the retention of the record.

We will not transfer any personal information across a country's border without your prior written consent. OR We may transmit or transfer personal information outside of the country in which it was collected to a foreign country and process it in that country. Personal information may be stored on servers located outside the country in which it was collected in a foreign country whose laws protecting personal information may not be as stringent as the laws in the country in which it was collected.

FAQs

1. Does POPIA apply to OpenUp as a non-profit organisation?

POPIA applies to us when we are *processing personal information*. There is no blanket exclusion from POPIA for when we are conducting research, for non-commercial activities, or even when using public data. The only forms of personal information processing that **are** excluded from POPIA are Personal Information –

- related purely to personal and household activities;

- that has been de-identified;
- related to “National security”;
- related to the functions carried out by Cabinet or the Judiciary; and
- used for journalistic, literary or artistic purposes (subject to any applicable Codes of Conduct).

These exclusions are unlikely to exist in any of OpenUp’s data processing practises.

There are exceptions, though, to certain conditions for processing within the sections themselves, and note the general exemption covered under our FAQ item “What happens if we’re processing data on behalf of a government department or municipality?” below.

2. When is OpenUp the responsible party?

We are the responsible party when we determine the process of, and means for, processing the personal information in question. It is important to remember given our work that when we process personal information we *are often acting as the operator* for clients, and then our obligations are different. Here is the simple test for checking if we are the *responsible party*:

A Responsible Party determines the purposes and means of the processing, i.e. the why and how of the processing.

3. When do OpenUp need to get your consent?

It is a common misconception that you must *always* have the consent of a data subject to process personal information. Consent is not a ‘condition’ for lawful processing. Rather, lawfulness is a condition of processing. Consent can be a grounds for establishing this lawfulness, and is specifically required only in certain instances.

The lawful processing limitation grounded in **section 11** outlines the specific situations where consent *may* be required for establishing lawfulness, such as for processing the personal information of a child, but also for processing data for the purpose of *direct marketing* (such as through newsletters, but the rules for direct marketing come from **section 69**). Vitally, POPIA states that Personal Information can be Processed if it protects the *legitimate interests* of the data subject, or if needed for purposes of carrying out a contract between the data subject and OpenUp. What constitutes a “legitimate interest” forms a significant part of GDPR jurisprudence (in other words the privacy cases based on Europe’s version of POPIA). Importantly for many of OpenUp’s activities, we do not need to directly obtain consent to process when the personal information is in the public domain.

Note though, even if processing to protect a legitimate interest, consent can still be withdrawn by a Data Subject at a later stage (unless there is a specific law applicable which says otherwise).

4. How should OpenUp gather consent properly?

If we are required to get consent, or wish to get consent as best practice, consent must be *explicit*, *informed* and *specific*:

- A person must have a choice whether to consent or not (it must be voluntary).
- There must be *an expression of will*, e.g. tick box etc. In a GDPR case, a *pre-ticked* consent box was held not to constitute adequate consent.
- GDPR case law shows that, for it to be real, you should be able to withdraw it without detriment.
- It must relate to a specific purpose (for example, to contact me about my request). You must specify your purpose. The specificity can be facilitated by the notice.
- You must notify the Data Subject of various things as set out in **section 18** of POPIA (so just because you don't need express consent, *doesn't mean notification mustn't happen*); and
- You must inform the person sufficiently to enable them to make a decision.

Those guides are what we use for our consent gathering, when it us undertaken.

5. Must we delete your personal data on their request?

It is important to remember that in South Africa there is no "right to be forgotten" in the sense as understood in *Google v Spain*, which was an EU decision around de-indexing. Data subjects have the rights prescribed in **section 5** (read with **section 24** in this case), which includes rights to the correction or deletion of personal information that is either: **Inaccurate; Irrelevant; Excessive; Out of date; Incomplete; Obtained unlawfully**; or that it is **no longer authorised to retain** in terms of **section 14**.

In interpreting **section 14**, it is worth highlighting that such time is determined by considering if retention is any longer necessary for achieving the purpose for which the personal information was collected and processed, and will be highly reliant on the originating statute or lawful purpose which led to that personal information being made public information (presuming here that it would relate to open data we had collected).

6. Must OpenUp de-index personal data on request?

Again it is also important to remember that in South Africa there is no "right to be forgotten" in the sense as understood in *Google v Spain*, which was an EU decision around de-indexing. See further the answer to the question above.

However, as an organisation that prides itself on forwarding access to information, and is deeply respectful of personal privacy rights, OpenUp will nevertheless, and at its own discretion, and only if reasonably technically possible, and always subject to the provisions of POPIA, consider an application for de-indexing of personal information on application where the Data Subject can show that there is

a *reasonable* and *demonstrable* belief that the disclosure would lead to an imminent and serious personal safety risk, or another form of serious and irreversible personal risk that arises from the nature of the Personal Information, and the details of the case itself. This will be determined while balancing against the fact that it will have already been established that this Personal Information is lawfully displayed (or else **section 14** would apply), as well as against the broader public interest in the information being easily searchable.

Just by way of explanation, OpenUp have included this additional protection on the basis of the understanding that there may be use cases we have not considered.

If a data subject is aggrieved by a decision to not correct or delete personal Information based on the listed grounds, a data Subject will be able to approach the Regulator, but **only on the basis of the breach of lawful processing conditions contained in Chapter 3 of POPIA** (i.e. not on the basis of this additional protection we have provided).

7. What happens if OpenUp is processing data on behalf of a government department or municipality?

OpenUp sometimes acts as an operator on behalf of public entities. While the Responsible Party is generally responsible for compliance, as operator we must maintain security safeguards. In this type of collaboration it is also worth noting that *specific exceptions* are provided in relation to the processing of personal information, when conducting processing for a public function that might be useful for you to know as a data subject.

Personal Information Processed for the purpose of discharging a relevant function is exempt from sections **11(3)** (i.e a Data Subject can't object to processing) and (4), **12** (i.e. you need not collect data directly from the Data Subject), **15** (i.e. you can further process differently from the original purpose of collection) and **18** (i.e. need not notify a Data Subject when collecting information) in any case to the extent to which the application of those provisions to the Personal Information would be likely to prejudice the proper discharge of that function.

"Relevant function" for purposes of subsection (1), means any function —

- of a public body; or
- conferred on any person in terms of the law; or
- which is performed with the view to protecting members of the public against financial loss due to dishonesty, malpractice, or other forms of serious improper conduct by persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or other professions.