POPI POLICY

1. What is POPIA?

The Protection of Personal Information Act (POPIA), also referred to as the POPI Act, aims to protect an individual's right to privacy regarding their personal information which may have been collected by a third party during a normal commercial transaction or by their HR department prior to, or during, the course of their employment. It also seeks to bring South African law regarding ensuring and managing personal data in line with international data protection laws.

2. What is the Objective of POPI?

The purpose of POPI is to regulate and formalise how companies collect, store, protect, access and distribute consumer information and to protect the ongoing integrity and sensitivity of that private information. The Act offers many safeguards regarding using an individuals' personal data, and primarily protects individuals from unsolicited emails & SMS's for services which they never applied for, as well as against any security breaches that could result in identity theft, when personal information is stolen or offered too freely by a third party.

3. Who is covered?

- ✓ Clients/ Consumers – regarding their buying habits, historic transactions, activities, etc.
- ✓ Suppliers – their pricing, contracts, contacts, etc.
- ✓ Employees – HR info, Payroll records, CV's, applications for employment, CCTV records, T & A records, performance reviews, IR records, emails, etc.

4. How does this affect Companies?

This Act will impact all companies who in their "normal course of business" collect, manage, manipulate, analyse, distribute, use, retrieve, store, retain, destroy, delete, or interrogate any form of personal data, be that data from a potential Employee, an existing Employee or a discharged / previously employed Employee.

In most cases companies have implemented measures to manage their HR related information in a secure environment by either using internal or cloud based software systems. One cannot however assume that these measures are necessarily sufficient to satisfy POPI, so it is imperative that as a responsible business owner / Employer / HR or Payroll Manager Reviews of internal procedures and controls must regularly be conducted to ensure compliance with the Act. This should include, amongst others, reviewing recruitment process and obtaining consent from suppliers and Employees before collecting and storing personal information.

The requirements as specified in the Gazette that covers Record Keeping as well as the ICT and Tax Administration Acts are integral to a company's ability to adhere to this Act. Companies need to

have an understanding of all these Acts and as such have an integrated approach when implementing POPI. The Act includes a section to do with managing Special Personal Information. This deals with, for example, information related to political, sexual, religious persuasion and information about children.

Personal data which is maintained across borders is also dealt with by the Act, specifically relating to countries where inadequate information protection frameworks exist, or where companies store their data in the cloud and the actual cloud infrastructure is actually resident in another country.

5. 8 Key POPIA Conditions

The Act contains 8 key conditions that an entity which intends to process personal information lawfully, must comply with:

1) Processing Limitation

We collect information directly from you where you provide us with your personal details, for example when you submit your CV, purchase a product or services from us or when you submit enquiries to us or contact us via our website. Where possible, we will inform you what information you are required to provide to us and what information is optional.

Examples of information we may collect from you are:

- *Your name*
- *Your address*
- *Your email address*
- *Your telephone/mobile number*
- *Any user-generated content, posts and other content you submit to our website*

Non-Personal Information:

We may also collect non-personal information about you from other sources, such as our website/ LinkedIn or other social media, in the event you have requested, queried products or services from us, or requested brochures as an example.

We may also at times and only when strictly necessary supply third parties with your information, ie: to our vendors that you may be receiving services/ support from, and only for that specific purpose.

2) Purpose Specific

RedBridge will use your Personal and Non-Personal Information only for the purposes for which it was collected or agreed with you,

Some examples:

- *To confirm and verify your identity or qualifications for a customer if you're being on-boarded as a consultant of ours*
- *For ant contractual agreements and obligations between you and us/ our clients*

- *To notify you about changes to our service*
- *For the detection and prevention of fraud, crime, or other malpractice*
- *To conduct market or customer satisfaction research or for statistical analysis*
- *For audit and record keeping purposes*
- *In connection with legal proceedings*
- *We will also use your Personal Information to comply with legal and regulatory requirements or industry codes to which we subscribe or which apply to us, or when it is otherwise allowed by law.*
- *For monitoring and auditing site usage*
- *Analyse the effectiveness of our advertisements, competitions and promotions*
- *Personalise your website experience, as well as to evaluate (anonymously and in the aggregate) statistics on website activity, such as what time you visited it, whether you've visited it before and what site referred you to it*
- *Collect information about the device you are using to view the site, such as your IP address or the type of Internet browser or operating system you are using, and link this to your Personal Information so as to ensure that the site presents the best web experience for you*
- *To contact you regarding products and services which may be of interest to you, provided you have given us consent to do so or you have previously requested a product or service from us and the communication is relevant or related to that prior request and made within any timeframes established by applicable laws.*
- *Offer you the opportunity to take part in competitions or promotions*
- *You can opt out of receiving communications from us at any time. Any direct marketing communications that we send to you will provide you with the information and means necessary to opt out.*
- *To respond to your queries or comments*
- *Where we collect Personal Information for a specific purpose, we will not keep it for longer than is necessary to fulfil that purpose, unless we have to keep it for legitimate business or legal reasons. In order to protect information from accidental or malicious destruction, when we delete information from our services we may not immediately delete residual copies from our servers or remove information from our backup systems.*

3) Further Process Limitation

We do not process any personal information, beyond the reasons required for it, and we do not change any information for any purpose.

We do not process any information beyond any contractual rights we may have with any Data subject.

4) Information Quality

We ensure that information we collect is complete, accurate, and does not misrepresent or data subjects, by updating the data we have regularly, and communicating directly with the data subject.

5) Openness

We have total transparency with our data subjects. Our data subjects are informed about:

- *Giving permission for the submission of their information, where necessary*
- *What information is required,*
- *Duration it is kept for,*
- *Point of contact at RedBridge*

6) Security Safeguards

RedBridge uses a cloud-based application for email communication, and storage and by default, this has its own security controls.

We have an IT Policy, Information Security Policy and security applications to ensure that your personal information is protected against unauthorised access, accidental loss, or destruction.

One of the applications we use is an anti-data exfiltration platform which prevents unauthorised information from leaving our laptops and devices, or nefarious process from running on them.

7) Individual participation

RedBridge Data subjects are informed that they can request at any stage the information we have on them. We also periodically contact data subjects to update information.

8) Accountability

We use recognized GRC experts in the industry to assist us in drawing up our policies and procedures in order to adhere to the act.

COOKIES:

What are cookies?

Cookies help your browser navigate a website and the cookies themselves cannot collect any information stored on your computer or your files. We use cookie technology on some parts of our website. A cookie is small pieces of text that are saved on your Internet browser when you use our website. The cookie is sent back to our computer each time you visit our website. Cookies make it easier for us to give you a better experience online. You can stop your browser from accepting cookies, but if you do, some parts of our website or online services may not work. We recommend that you allow cookies.

- **Why do we use cookies?**

  We use cookies to learn more about the way you interact with our content and help us to improve your experience when visiting our website. Cookies remember the type of browser you use and which additional browser software you have installed. They also remember your preferences, such as language and region, which remain as your default settings when you revisit the website.

Cookies may also allow you to rate pages and fill in comment forms.

- **What cookies do we use?**
    - session cookies - only last until you close your browser,
    - persistent cookies - which are stored on your computer for longer,
    - third party cookies- also referred to as tracking cookies, collects data based on your online behavior

- **How are third party cookies used?**

For some of the functions within our websites we use third party suppliers, for example, when you visit a page with videos embedded from or links to YouTube. These videos or links (and any other content from third party suppliers) may contain third party cookies and you may wish to consult the policies of these third-party websites for information regarding their use of cookies.

- **How do I reject and delete cookies?**

We will not use cookies to collect personally identifiable information about you. However, should you wish to do so, you can choose to reject or block the cookies by changing your browser settings as per our website.

Please note that most browsers automatically accept cookies so if you do not wish cookies to be used you may need to actively delete or block the cookies. You can also visit www.allaboutcookies.org for details on how to delete or reject cookies and for further information on cookies generally.

For information on the use of cookies in mobile phone browsers and for details on how to reject or delete such cookies, please refer to your handset manual. Note, however, that if you reject the use of cookies you will still be able to visit our website but some of the functions may not work correctly.

Information Regulator

An Information Regulator has been appointed by the President on the recommendation of the National Assembly and is answerable to the National Assembly. There will be a large body of staff working under the Information Regulator.

The Information Regulator's duties are varied, and he/ she has the power and authority to handle all matters relating to the POPIA Act.

The Information Regulator must immediately be advised in the event of a breach which resulted in Personal Information falling into the wrong hands.

Guidance notes on requests for information, disputes and complaints can be with the Information Regualtor as per details below.

- Home - Information Regulator (inforegulator.org.za)
- Tel: 010 023 5200
- Email: enquiries@inforegulator.org.za