



## Privacy Policy (POPIA)

### 1. Introduction

In line with the Protection of Personal Information Act, 2013 (POPIA) (**'the Act'**) and its recognition:

Section 14 of the Constitution of South Africa, 1996, provides that everyone has the right to privacy; and that the right to privacy includes protection from unlawful collection, retention, dissemination, and use of personal information.

iFacts (Pty) Ltd and its affiliates (**"the Company"**) acknowledges and embraces its duty to comply with the provisions of the Act by:

- 1.1. Respecting the right to privacy of natural and juristic persons;
- 1.2. Sourcing, storing, processing, and retaining personal information by ethical and lawful means only.

### 2. Scope of Policy

This policy is applicable to all employees, directors and shareholders of the Company. It also applies to users accessing the iFacts website, including specific sections such as the Ad Hoc Enquiry page at <https://www.ifacts.co.za/adhocenquiry.php>.

The collection, processing, and retention of personal information through the website will be handled in compliance with the POPIA and the principles outlined in this policy.

### 3. Purpose and Application

The purpose of this policy is to incorporate, implement, and apply the provisions of the Act into the operations of the Company.

- 3.1. To safeguard personal information;
- 3.2. To regulate the processing of personal information.

### 4. Definitions

- 4.1. **Child:** A natural person under the age of 18 who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him/herself.
- 4.2. **Consent:** Any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.



- 4.3. **Competent person:** Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
- 4.4. **Data subject:** The person to whom the personal information relates.
- 4.5. **Direct marketing:** Approaching a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
  - 4.5.1. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
  - 4.5.2. Requesting the data subject to make a donation of any kind for any reason.
- 4.6. **Electronic communication:** 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.
- 4.7. **Filing system:** Any structured set of personal information, whether centralized, decentralized, or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
- 4.8. **Information officer:** In relation to a public body: an information officer or deputy information officer as contemplated in section 1 or 17; or in relation to a private body: the head of a private body as contemplated in section 1 of the Promotion of Access to Information Act.
- 4.9. **Operator:** A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- 4.10. **Person:** A natural person or a juristic person.
- 4.11. **Personal information:**
  - 4.11.1. Information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including but not limited to:
  - 4.11.2. Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, color, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;
  - 4.11.3. Information relating to the education, medical, financial, criminal, or employment history of the person;
- 4.12. Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier, or other particular assignment to the person;
  - 4.12.1. The biometric information of the person;
  - 4.12.2. The personal opinions, views, or preferences of the person;



- 4.12.3. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  - 4.12.4. The views or opinions of another individual about the person; and
  - 4.12.5. The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
- 4.13. Processing: Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
- 4.13.1. The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
  - 4.13.2. Dissemination by means of transmission, distribution, or making available in any other form; or
  - 4.13.3. Merging, linking, as well as restriction, degradation, erasure, or destruction of information.
- 4.14. Promotion of Access to Information Act: The Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).
- 4.14.1. Public record: A record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
- 4.15. Record: Any recorded information:
- 4.15.1. Regardless of form or medium, including:
  - 4.15.2. Writing on any material;
  - 4.15.3. Information produced, recorded, or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded, or stored;
  - 4.15.4. Label, marking, or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
  - 4.15.5. Book, map, plan, graph, or drawing;
  - 4.15.6. Photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
  - 4.15.7. In the possession or under the control of a responsible party;
  - 4.15.8. Whether or not it was created by a responsible party; and
  - 4.15.9. Regardless of when it came into existence.
- 4.16. Regulator: The Information Regulator established in terms of section 39.
- 4.17. Responsible party: A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.



- 4.18. Special personal information: Personal information as referred to in section 26.
- 4.19. Unique identifier: Any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

## 5. Duties of the Information Officer and Compliance

### 5.1. An Information Officer's duties include:

- 5.1.1. Encouraging compliance by the body with the conditions for the lawful processing of personal information;
- 5.1.2. Dealing with requests made to the organization pursuant to the Act;
- 5.1.3. Working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the organization;
- 5.1.4. Otherwise ensuring compliance with the provisions of the Act and as prescribed.

### 5.2. There are eight (8) conditions that shall apply and are relevant for the lawful processing of personal information:

- 5.2.1. Accountability;
- 5.2.2. Processing limitation;
- 5.2.3. Purpose specification;
- 5.2.4. Further processing limitation;
- 5.2.5. Information quality;
- 5.2.6. Transparency (honesty and integrity);
- 5.2.7. Security safeguards; and
- 5.2.8. Data subject participation.

## 6. Collection and Processing of Personal Information

6.1. **Website Collection and Use:** Personal information may be collected when users access the iFacts website, including when they submit forms, queries, or other information through specific pages such as the Ad Hoc Enquiry page. The types of personal information collected may include but are not limited to names, contact details, IP addresses, and any information voluntarily provided by the user.

6.2. **User Consent:** By accessing the iFacts website, users consent to the collection and processing of their personal information as described in this policy. Specific consent will be sought for the collection of sensitive personal information or when required by law.



- 6.3. **Purpose of Collection:** Personal information collected via the iFacts website will be used for responding to queries, providing services, enhancing user experience, and other legitimate business purposes related to iFacts operations. Users will be informed of the specific purposes of data collection, particularly when submitting information through forms or enquiry pages.
- 6.4. **Data Security and Retention:** iFacts is committed to securing the integrity and confidentiality of personal information collected through its website by implementing appropriate, reasonable technical, and organizational measures. Personal information will not be retained for longer than necessary and will be securely destroyed or deleted when no longer required.
- 6.5. **User Rights:** Users have the right to access, correct, and delete their personal information collected through the iFacts website. Requests for such actions can be directed to the iFacts Information Officer. Users may withdraw their consent for the processing of their personal information at any time, subject to the conditions of lawful processing prior to the withdrawal.
- 6.6. **Website Cookies and Tracking:** The iFacts website may use cookies and other tracking technologies to enhance user experience and gather data on site usage. Users will be informed of the use of cookies and, where applicable, will be provided with options to manage their cookie preferences.
- 6.7. The procedure of processing personal information refers to the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, including inaccessibility, erasure or destruction of personal information.
- 6.8. Personal information collected by the Company and/or any of its representatives or subsidiaries will not be collected directly from the data subject unless:
- 6.8.1. The information is contained or derived from a public record or has deliberately been made public by the data subject.
  - 6.8.2. The data subject or a competent person where the data subject is a minor has consented to the collection of the information from another source.
  - 6.8.3. Collection of the information from another source would not prejudice a legitimate interest of the data subject.



- 6.8.4. Collection of the information from another source is necessary to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution, and punishment of offences; to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue; for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; in the interest of national security; or to maintain the legitimate interests of the Company or of a third party to whom the information is supplied.
- 6.8.5. Compliance would prejudice a lawful purpose of the collection.
- 6.8.6. Compliance is not reasonably practicable in the circumstances of that instance.
- 6.8.7. Personal information must only be collected for a specific, explicitly defined, and lawful purpose related to the function or activity of the Company.
- 6.9. Ensure that the data subject is aware of what information is collected prior to the collection thereof.
- 6.10. Ensure the data subject, or should the individual be a minor, a competent person in this instance, consents to the collection of personal information.
- 6.11. Inform the data subject what the purpose is for the collection of this information and inform the data subject regarding:
- 6.12. Whether the information to be collected is a voluntary or mandatory function to be performed;
- 6.13. The consequences for the data subject should they fail to provide the information;
- 6.14. Whether a legal authority requires the collection of the information for their records;
- 6.15. Whether this information needs to be transferred to another source;
- 6.16. Whether the company intends to transfer the information to any other country outside the borders of the Republic of South Africa or to an international organization, and disclose the level of protection regarding the personal information which can be expected from this country or international organization.
- 6.17. Ensure that the personal information is complete, accurate, not misleading, and is updated from time to time.
- 6.18. Ensure that the information collected is not excessive. Only collect the information necessary for the Company to execute its functions or in the interests of a third party to whom the information will be provided.



- 6.19. Undertake to regard personal information as strictly private and confidential and not to disclose it to any other party unless required by law to do so or for the proper performance of the company's duties and tasks.
- 6.20. The Company will take responsibility for keeping on record all appropriate documentation of all processing operations.
- 6.21. The Company undertakes to ensure that any additional processing of personal information will be in accordance with the purpose for which it was collected.
- 6.22. To assess whether any additional processing is in accordance with the purpose of collection, the following details should be considered:
  - 6.22.1. The relationship between the purpose of the intended additional processing and the purpose or intention for which the information was collected;
  - 6.22.2. The nature of the information concerned;
  - 6.22.3. The consequences of this action for the data subject regarding the intention of processing additional information;
  - 6.22.4. The manner/method in which this information was collected; and
  - 6.22.5. Any contractual rights and obligations between the parties.

## **7. Direct Marketing**

The processing of personal information of a data subject for the purpose of direct marketing by electronic means is prohibited unless the data subject:

- 7.1.1. Has given consent; or
- 7.1.2. Subject to subsection 3 of the Act, is a customer of the organization.
- 7.1.3. An organization may approach a data subject for the purpose of obtaining consent if consent was not previously withheld.

## **8. Retention of Records**

- 8.1. Records of personal information should not be retained for longer periods than is necessary for achieving the purpose for which the information was collected unless:
  - 8.1.1. The retention of a record is required or authorized by law;
  - 8.1.2. The Company reasonably requires a record for legal purposes related to its functions or activities;
  - 8.1.3. Retention of a record is required by a contract between the parties thereto; or
  - 8.1.4. The data subject or a competent person, where the data subject is a minor, has consented to the retention of a record.



- 8.2. The Company will destroy or delete a record of personal information as soon as it is reasonably practical once it has no further authority to retain the record.
- 8.3. The deletion of a record of personal information should be processed in a manner that prevents its reconstruction in an intelligible/understandable form.
- 8.4. In the event that the Company uses a record of personal information from a data subject to arrive at a conclusion regarding various aspects pertinent to the data subject, the following will be necessary:
  - 8.4.1. Retain the record for such period as may be required or prescribed by law or a code of conduct; or
  - 8.4.2. If there is no law or code of conduct prescribing a retention period, retain the record for a period that will afford the data subject a reasonable opportunity to request access to the record, taking all considerations relating to the use of the personal information into account.
- 8.5. The Company will restrict the processing of personal information if:
  - 8.5.1. Its accuracy is contested by the data subject, for a period enabling the Company to verify the accuracy of the information;
  - 8.5.2. The Company no longer requires the personal information for achieving the purpose for which it was collected or subsequently processed, but is required to maintain/retain it for purposes of proof or record-keeping;
  - 8.5.3. The processing is unlawful, and the data subject opposes its destruction or deletion and alternatively requests the restriction of its use; or
  - 8.5.4. The data subject requests that the personal data be transmitted or transferred to another automated processing system.
  - 8.5.5. Personal information that has been restricted may only be processed for purposes of proof, with the data subject's consent or with the consent of a competent person where the data subject is a minor, or for the protection of the rights of any other natural or legal person, or if such processing is in the public interest.
- 8.6. Where personal information is restricted, the Company will inform the data subject prior to the termination of the restriction.





## **9. Security of Information**

- 9.1. The Company will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical, and organizational measures to prevent the loss of, damage to, or unauthorized destruction of personal information; and unlawful access to or processing of personal information.
- 9.2. The Company will take responsible measures to:
  - 9.2.1. Identify all reasonably predictable internal and external risks to personal information in its possession or under its management;
  - 9.2.2. Establish and maintain appropriate safeguards against the risks identified;
  - 9.2.3. Regularly verify that the safeguards are effectively implemented; and
  - 9.2.4. Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguarding methods.
- 9.3. The Company will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

## **10. Security Breaches**

- 10.1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person, the information officer should be contacted immediately.
- 10.2. The information officer is required to notify the Information Regulator and the data subject.
- 10.3. The notification of a breach of confidentiality should be declared as soon as is reasonably possible upon the discovery of the compromise.
- 10.4. The information officer needs to provide sufficient information to the data subject to enable them to take protective measures against the potential consequences of the compromise.

## **11. Complaints to the Information Regulator**

- 11.1. Any person or employee may submit a complaint to the Regulator.
- 11.2. The complaint must be made in writing.



## 12. Rights of Data Subject

- 12.1. The data subject, or a competent person where the data subject is a minor, may withdraw their consent to procure and process their personal information at any time, provided that the processing of the personal information was performed legally prior to the request for withdrawal.
- 12.2. A data subject, having provided adequate proof of identity, has the right to:
  - 12.2.1. Request the Company to confirm, free of charge, whether it holds personal information regarding the data subject; and
  - 12.2.2. Request from the Company a record or a description of the personal information relevant to the data subject held by the Company, including information regarding the identity of all third parties or categories of third parties who have or have had access to the information.
  - 12.2.3. This must be processed within a reasonable period, at a fee prescribed as determined by the Information Officer, in a reasonable manner and format, and in a form that is generally understandable.
  - 12.2.4. A data subject may request the Company to correct or delete personal information in its possession or under its management which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or has been obtained illegally;
  - 12.2.5. A data subject may request the Company to destroy or delete their record of personal information. This must be processed only if it is permissible and has been approved by the Information Officer.

## 13. Implementation and Monitoring

- 13.1. All employees will be responsible for administering and overseeing the implementation of this policy, including supporting guidelines, standard operating procedures, notices, consents, and appropriate related documents and processes.
- 13.2. Employees who violate the guidelines and standard operating procedures of this policy may be subjected to disciplinary action.



#### 14. Information Regulator and Information Officer

14.1 Information Regulator  
Address: JD House, 27 Stiemens Street, Braamfontein,  
Johannesburg, 2001  
P.O. Box 31533, Braamfontein, Johannesburg, 2017  
Complaints email: [complaints.IR@justice.gov.za](mailto:complaints.IR@justice.gov.za)  
General enquiries email: [infoereg@justice.gov.za](mailto:infoereg@justice.gov.za)

14.2 iFacts Information Officer  
Information Officer: Monique Beetge  
Email: [info@ifacts.co.za](mailto:info@ifacts.co.za)  
Deputy Information Officer: N/A  
Email: N/A