THE DIGITAL LAW CO
BY EMMA SADLEIR
www.thedigitallawco.com +27(0)83-565-5683 info@thedigitallawco.com @emmasadleir

CONFIDENTIAL

MEMORANDUM TO PROJECTS IQ

INTRODUCTION

1. We have been requested to provide Projects IQ (Pty) Ltd ("**the Company**") on the law of data protection in South Africa, in particular the Protection of Personal Information Act No. 4 of 2013 ("**POPI**").

2. We are instructed that the Company is a subscription-based mining information and reporting service ("**the Service**"). We are further instructed that the nature of this service requires the Company to collect and process the information of its users via the website www.africaminingiq.co.za ("**the Website**").

3. We record that this memorandum is limited solely to POPI. Should the Company have users based in the European Union, the Company may have to adhere to the General Data Protection Regulations ("**GDPR**") which came into effect on the 25 May 2018, we may have to provide a supplementary memorandum. We further record that this memorandum is limited solely to processing of information of users of the Website as obtained by the company in the course and scope of its services. It does not apply to processing of internal company human resources information, corporate communication and record management, which once POPI is in full force and effect, will also need to be POPI compliant.

BACKGROUND AND PURPOSE OF POPI

4. Data protection is a branch of the law relating to the protection of privacy. Every South African citizen is entitled to the right to privacy under Section 14 of the Constitution. Data protection involves safeguarding a person's information where it is collected, stored, used or communicated by another person or institution. Data protection in South Africa is governed by POPI which has not yet been commenced in its entirety.

5. The digital age presents extensive data protection concerns, particular as people's attitudes to their personal information, and the commodification of that information, change. The digitisation of information has seen a marked rise in the processing of personal information: not only is more personal information generated, but it is easier to access, store, edit, circulate and duplicate. In line with a worldwide movement to better regulate this increased processing of personal information, both on and offline, as well as in recognition of the value that personal data holds in the digital age and the resultant necessity to protect the privacy of individuals, the POPI Act was signed into law on 26 November 2013.

6. POPI provides a general information protection mechanism, which is applicable to both the public and private sector and will, in future, be supplemented by codes of conduct for the various sectors. POPI covers both automated and manual processing of information and will protect identifiable natural and juristic persons. POPI establishes a juristic person known as the Information Regulator ("**the Regulator**"), whose duties include the monitoring and enforcing of compliance to the Act.

7. The primary basis on which to found the lawful processing of personal information in terms of the POPI Act is by way of consent of the data subject.[1] Consent is defined in section 1 of POPI as "*any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information*".

INFORMATION PROCESSING BY WEBSITES

8. The extent to which websites collect and aggregate user data is increasingly controversial. Not only does this practice present significant challenges to an individual's effective control over his or her personal data[2], but there are arguments that users do not fully appreciate the extent to which their personal information is collated, used or shared by social media websites.

[1] Sections 11(1)(a) and 27 of the POPI Act.

[2] EC Commission Communication. See also London Economics "Study on the economic benefits of privacy-enhancing technologies (PETs): Final Report to the European Commission, DG Justice, Freedom and Security" (July 2010) (retrieved from (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf) at 14.

9. The issue is a complex one, to which no clear solutions have been provided. In a South African context, the lawfulness of the extent to which personal information is processed by websites has not been considered. Once in full force, POPI is expected to have an impact on this processing and will provide a statutory stick with which the newly-formed Information Regulator will be able to investigate and fine responsible parties who fail to comply with the provisions of the Act insofar as its information processing practices are concerned.

IMPLEMENTATION OF POPI

10. A few limited sections of POPI have already commenced, but the majority of POPI (especially the sections that create compliance requirements) will only commence on a later date to be proclaimed by the President. The commencement date will be before the end of December 2018. Bear in mind that there is a one-year grace period for compliance - that runs from the commencement date (i.e. compliance with POPI is required by the end of the grace period).

DUTIES OF THE COMPANY AS DETAILED IN POPI

11. Prior to discussing the relevant provisions of POPI, it is necessary to understand some of the key definitions:

- "**personal information**" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including but not limited to:
    - information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual,
    - information relating to the education or the medical, financial, criminal or employment history of the person;
    - any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;

- the biometric information of the person (for example, fingerprints and voice recognition);
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private confidential nature or further correspondence that reveals the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- 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.

- "**processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
  - the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
  - dissemination by means of transmission, distribution or making available in any other form; or
  - merging, linking as well as blocking, degradation, erasure or destruction of information;

- "**data subject**" means the person to whom personal information relates;

- "**consent**" means any voluntary, specific and informed expression of will, in terms of which a data subject agrees to the processing of personal information relating to him or her;

- "**responsible party**" means a public or private body or any person which, alone or in conjunction with others, determines the purpose of a means for processing personal information;

12. In processing personal information, the responsible party is required in terms of POPI to adhere to the eight conditions for lawful processing of personal information:

12.1 **Condition 1: the accountability principle.**

- The first principle requires that a responsible party be accountable for complying with measures which give effect to the 8 data protection principles.

12.2 **Condition 2: limitation**

- The second principal limits the processing of personal information in the following way:
    - the collection of personal information must be lawful -- in other words there must be lawful justification for the process;
    - the purpose for the processing of personal information must be relevant and adequate for the purposes for which it is required, and the personal information must be complete, accurate, and up to date;
    - personal information must be collected directly from the data subject unless collection from a third party is authorised, or it is contained in the public record.

12.3 **Condition 3: purpose specification**

- The third principle provides that the purposes for which personal information is collected must be specified and communicated to the data subject, not later than at the time of collection. Thereafter, personal information may not be retained any longer than is

strictly necessary for achieving the purpose for which the personal information was collected.

12.4 **Condition 4: further processing limitation**

- Subsequent use of the personal information can only take place in compliance with the original purpose of collection. Accordingly, personal information cannot be disclosed, made available or otherwise used for any purposes other than those specified in accordance with the original purpose for which the information was collected, except in the following circumstances: (i) with the consent of the data subject; or (ii) by the authority of law.

12.5 **Condition 5: information quality**

- The responsible party is required to take reasonable steps to ensure that the personal information held, is accurate, complete, not misleading and is kept up to date.

12.6 **Condition 6: openness**

- Personal information may only be processed by a party that has notified the **Regulator.** The responsible party is also required to inform the data subject of circumstances surrounding the processing of their personal information.

12.7 **Condition 7: security safeguards**

- The responsible party is required to put in place reasonable security safeguards to ensure that personal information is protected against risks such as loss, unauthorised access, destruction, use, modification or disclosure of data.

12.8 **Condition 8: data subject participation**

- A data subject is entitled, upon proof of identity, to:

- obtain from the responsible party, confirmation of whether or not the responsible party has personal information relating to them;
- request a description of the personal information held by the responsible party;
- request information on or about all parties who have had access to the data subject's personal information;
- contest the content of the personal information held by the responsible party, and if successful have the personal information you raised, rectified, completed or amended.

CONSEQUENSES FOR FAILURE TO COMPLY WITH POPI

13. Any person may lodge a complaint with the Regulator, after which the Regulator will go through the following steps:

- The Regulator may try to secure a settlement between the parties
- In the event that no settlement is possible, the Regulator may try and secure settlement
- If there is a breach the Regulator may issue enforcement notice
- The data subject / Regulator may sue the responsible party for damages.
- The processor may also face between one to ten years imprisonment, a R10 000 000 fine, or both.

LAWFUL PROCESSING BY THE COMPANY UNDER POPI

14. POPI will apply to the processing of personal data by the Company and the Company will be considered a responsible party. Users of the Website would be considered data subjects vis-à-vis the processing of their data. In order to comply with the lawful processing requirements of POPI, we advise that the Company complies with the following minimum requirements:

14.1 Information process audit: The Company should conduct an internal audit on the processes used to collect, record, store, disseminate and destroy personal information. The Company must specifically ensure the integrity and safekeeping of personal information in its possession or under its control. Assess whether information is at risk of being lost or damaged, duplicated or unlawfully accessed, and take steps to guard against such risk.

14.2 Classify information: The Company will need to know exactly which of the data contains personal information, determine why it is being retained, and define how long it needs to be kept. If the information in question is not essential to the Company's operations (for example, contacts of old clients), earmark it for deletion.

14.3 Obtain user consent: All users of the Service need to give the Company consent for the company to process their personal information. This consent must be given freely by agreeing to the **Terms and Conditions** and **Privacy Policy**. The Company must provide comprehensive and clear information about the purposes and different ways in which they intend to process or use personal data at the time that the data is collected i.e. exactly what the Company is going to do with the information must be explained to the user on sign-up. This is addressed in the Company's newly drafted Privacy Policy. It is noteworthy that subsequent use of the personal information can only take place in compliance with the original purpose of collection (the personal information obtained cannot be used for any other purpose in the future).

14.4 Destroy unnecessary information: In line with the "purpose specification" condition, the Company should be to procure the services of a reputable service provider to destroy all personal information that it does not need. Both digital and physical files need to be processed by a reputable document destruction service, in order to guarantee that no information is compromised.

14.5 Set maximum periods: The Company must set maximum periods to retain the information, which cannot be held for any longer than is strictly necessary for achieving the purpose for which the personal information was collected.

14.6 Communicate policy and process changes with clients. In line with the "purpose specification" condition, the Company must notify its data subjects, where, how and why their data is being stored. This information will be covered by the Company's newly drafted Privacy Policy. For new clients using the Services once the new Privacy Policy is in effect, consent to the Privacy Policy will be a pre-requisite for using the Services, however, the Company will need to ensure that all existing clients read and consent to the new and updated Privacy Policy.

14.7 Set up systems to accommodate data subject requests: the POPI allows data subjects to make certain requests, free of charge, to organisations holding their personal information. For instance, the data subject has the right to know the identity of all third parties that have had access to their information. A data subject can also ask for a record of the information concerned.

14.8 Inform the regulator: When POPI's compliance provisions come into force, the Company must notify the Information Protection Regulator that it is processing personal information.

14.9 Implement security safeguards: The personal information must be safely secured and the Company must put in place reasonable security safeguards to ensure that personal information is protected against risks such as loss, unauthorised access, destruction, use, modification or disclosure of data. It is worth noting that the Regulator will require all companies need to commit to annual reassessments of their information systems.

14.10 Check the rationale for any further processing: if any personal information is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was initially collected.

14.11 Ensure that direct marketing complies with POPI: POPI contains specific provisions on the way in which companies may go about direct marketing (which includes both electronic marketing and marketing by other means). Direct marketing must:

14.11.1 Comply with 8 processing conditions;

14.11.2 Contain details of the sender or the person on whose behalf the information is sent; and

14.11.3 Contain and address of contact details to opt out.

It is recommended that the Company procure the services of an expert service provider to guide it through its POPI-compliance process.

Please do not hesitate to contact us should you have any further queries.

EMMA SADLEIR / SARAH HOFFMAN

THE DIGITAL LAW CO

25 May 2018