PROTECTION OF PERSONAL INFORMATION

Into Africa ascribes to the information protection ideals enshrined in the European General Data Protection Regulation ("GPDR"), which in our South African context means compliance with the Protection of Personal Information Act 4 of 2013 ("POPI"). Although not yet in effect, we have elected to voluntarily comply with the provisions of POPI pending its effective date. In doing so, we are committed to adhere to the following core principles:

1. **Accountability**
   This means that we ensure that we comply with the information protection principles and requirements of POPI during the entire process of gathering, classifying and processing personal information.

2. **Processing limitation**
   We collect and process personal information:
   - Only for a legitimate purpose
   - Only to the extent that such information is *relevant*, *adequate* and *not excessive* in relation to our services
   - Only once, and for as long as, we have the proper consent and authorization to do so
   - Directly from the individual to which it relates, unless they have authorized an intermediary to share such information with us

3. **Purpose specification, retention and restriction of records**
   - We collect and process personal information for the specific purpose of rendering our advertised services. This may include retaining a minimum amount of personal information that enables us to interact with clients in the future.
   - We retain personal information only for as long as it is reasonably required to do so for the purpose for which it was obtained, or as prescribed by law.
   - We restrict access to personal information if:
     - Its accuracy is contested by the person to which it relates, until the accuracy issue can be resolved
     - The purpose for retaining such information has expired, but we are required to retain the records for purposes of proof
     - The processing of the information was unlawful, but the person to which it relates has requested us to restrict access instead of destroying it
     - The person to which the information relates has requested that we transmit it to a third party automated processing system

4. **Limitation on further processing**

   The personal information processed by us is only used for the purposes described above, or for a purpose compatible with those purposes. Generally speaking, this means that we only use it in relation to the services that we render and to maintain and update our client database.

5. **Information quality**

We are reliant on the individuals to whom personal information processed by us relates to guarantee the accuracy of the information that they provide to us, as this is impossible for us to verify independently in most cases. However, we do take active steps to verify such information with such individuals if we encounter a patent error or suspected inaccuracy. Our physical and electronic information storage systems also ensure, to the reasonable extent required, that information integrity is not compromised.

6. Openness

We keep a record of our company details and a description of the types of information that we deal with, which may be accessed by the public in accordance with prescribed procedures (governed by the Promotion of Access to Information Act 2 of 2000)

We also notify the persons to whom personal information processed by us relates that we are collecting such information, and of a number of other prescribed details. Sometimes this notification will be done by an intermediary dealing directly with such persons, in which case they will obtain the written consent of such persons to share such information with us.

7. Information security

We are required to secure the integrity and confidentiality of personal information in our possession or under our control by taking appropriate, reasonable technical and organisational measures by having due regard to generally accepted information security practices and procedures. In practice we do this by restricting access to our physical records to trusted individuals, such as our employees, and by voluntarily implementing, to the best of our ability, the UK National Cyber Security Centre's recommendations on cyber security for small businesses (visit https://www.ncsc.gov.uk/ for more information).

When we deal with third party operators, such as sub-contractors, we ensure that personal information in our possession is provided to them only with our knowledge and subject to legally binding agreements requiring them to keep such information confidential and subject to the same information security measures that we are required to adhere to.

In the event of a data breach, we will inform the relevant authorities and the person to which the compromised information relates as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of our information system.

8. Data subject participation

As required, we provide confirmation to any person, free of charge, whether or not we hold personal information relating to them. We will also, on request, and subject to our right to require the payment of a prescribed fee, provide copies or a description of the actual records held by us. Access to such information is subject to the legal requirements and processes set out in the Promotion of Access to Information Act 2 of 2000.

Any person whose personal information we hold may request that we:

- Correct or delete any such information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully
- Destroy or delete any such information that the we are no longer authorised to retain

Issued by Nick Buckland, Director of Into Africa – April 2018