ENDCODE

Tech. Law. Policy. Africa.

Prepared for: **KPI**

Lens Limited

Prepared by:

Daniel Batty, EndCode

kpilens

DATA PROCESSING AGREEMENT

Entered into by and between

KPI Lens Pty Ltd

(Registration No:_________________)

("**KPI Lens**" **/** "**the Data Processor**")

and

____

(Registration No:______________________________)

("**the Data Controller**")

(collectively, "**the Parties**")

INTRODUCTION

This Data Processing Agreement ("DPA") outlines the various terms applicable to Processing activities conducted by and between KPI Lens and the Data Controller.

KPI Lens is a Data Processor which provides a software solution to the Data Controller which processes Personal Information for the purposes specified in this Agreement.

This Agreement is applicable to all other agreements and arrangements between KPI Lens and the Data Controller. Should there be any conflict between the provisions of any other agreement, including the Software as a Service Agreement and this Agreement, this Agreement takes precedence.

1. DEFINITIONS

The following expressions shall bear the meanings assigned to them below and cognate expressions shall bear corresponding meanings.

1.1. "**Agreement**" shall mean this Data Processing Agreement together with any amendments or annexures.

1.2. "**Analytics**" shall mean the collection, discovery and interpretation of meaningful observations, occurrences or patterns in User behaviour on KPI Lens Software. Analytics do not contain any Personal Data.

1.3. "**Authorised User/s**" means the natural person/s who are appointed by the Data Controller and who are empowered to exercise administrative privileges over the Platforms and the Software.

1.4. "**Data**" shall mean all information, including Personal Data, Processed by KPI Lens on behalf of the Data Controller, but shall not include Analytics.

1.5. "**Data Protection Laws**" shall mean any legislation protecting the fundamental rights and freedoms of individuals in respect of their right to privacy with respect to the Processing of Personal Data, including any other data protection policies, guidelines and/or procedures of the Data Controller which may be relevant. The specific Data Protection Laws relevant to the Data Controller are contained in Annexure 1 "Data Protection Law".

1.6. "**Data Controller**" shall mean a person who either alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which Personal Data is processed or is to be processed. For the purposes of this Agreement, the Data Controller shall refer to ________________________________

1.7. “**Data Processor**” shall mean, in relation to Personal Data, any person other than an employee of the Data Controller who processes the Personal Data on behalf of the Data Controller. For the purposes of this Agreement, the Data Processor refers to KPI Lens.

1.8. “**Data Subject/s**” shall mean any person to whom Personal Data relates.

1.9. “**Parties**” shall mean a reference to either the Data Controller or KPI Lens depending on the context.

1.10. “**Personal Data**” shall be defined in Annexure 1 in accordance with the prevailing and relevant Applicable Data Protection Law.

1.11. “**Process/Processing**” shall be defined in Annexure 1 in accordance with the prevailing and relevant Applicable Personal Data Protection Act.

1.12. “**Processing Instruction**” shall mean any actions relating to the Processing of Personal Information by KPI Lens, in relation to the Services from time to time;

1.13. “**Sevice/s**” shall mean the broad category of monitoring and evaluation services provided through a web-based platform. The monitoring and evaluation includes the development of automated reports according to pre-selected categories across multiple ongoing projects.

1.14. “**Security Compromise**” any intentional or unintentional breach of Personal Data in the possession of either Party.

1.15. “**Software**” shall mean KPI Lens’ Operational Intelligence solution, ‘KPI Lens’, a web-based application — accessible at: ***https://office.kpilens.com*** and through which the Data Controller access the Services.

1.16. “**Thid-Party”** shall mean any other person that is neither the Data Controller nor the KPI Lens. In the context of this DPA, Third-Parties may refer to Third-Party Data Processors, or Third-Parties who are not authorised to Process Personal Data.

2. ROLES AND RESPONSIBILITIES

2.1. Considering the applicable Data Protection Laws and the relationship between the Parties, the Parties agree and acknowledge that ____________________________ is the Data Controller and has appointed KPI Lens as its Data Processor, subject to instruction from the Data Controller, to provide the Services.

3. TERM AND APPLICATION OF THIS AGREEMENT

3.1. This Agreement shall be enforceable against both Parties until the end of the provision of the Services, which period shall include periods of suspension or other post-termination periods where the Data Processor continues to process Data on behalf of the Data Controller.

3.2. This Agreement shall apply to all directors, employees, subcontractors, agents and other personnel members of the Data Controller and the Data Processor.

4. SUBJECT MATTER AND CIRCUMSTANCES OF DATA PROCESSING

4.1. By entering this Agreement, the Data Controller instructs the Data Processor to Process the Data for the purpose of:

4.1.1. providing the Services, including all functionalities of the Software and all related operational and technical support relating to the Software; or

4.1.2. as further documented in Annexure 2 “Processing Instruction”.

4.2. The Data Processor will Process the Data until the expiry of the Agreement or until the Data Controller or a Data Subject objects to the Processing of the Data. The Data Processor will comply with the instructions of the Data Controller and will Process the Data in accordance with the Agreement.

4.3. When the Data Controller uses or receives the Services:

4.3.1. The **categories of Personal Data** listed in Annexure 2 “Processing Instruction” will be delivered to and Processed by the Data Processor

4.3.2. Personal Data pertaining to **categories of Data Subjects** listed in Annexure 2 “Processing Instruction” will be Processed by the Data Processor:

5. LAWFUL BASIS FOR PROCESSING OF PERSONAL DATA

5.1. The Data Controller’s instructions to the Data Processor shall comply with applicable Data Protection Laws. In this regard, The Data Controller shall establish the relevant Data Protection Law in Annexure 1 “Data Protection Law” and ensure that it has all required legal bases in order to:

5.1.1. collect, Process and transfer to the Data Processor any Personal Data contained in the Data; and to

5.1.2. authorise the Processing of Personal Data, by the Data Processor, on the Data Controller’s behalf.

5.2. Where Data Controller has obtained consent to collect and Process Personal Data, the Data Controller represents and warrants to the Data Processor that:

5.2.1. such consent was freely given by each of the Data Subjects and obtained in accordance with applicable Data Protection Laws;

5.2.2. such consent has not been withdrawn;

5.2.3. the Data Subject(s) have not objected to the transfer of their Personal Data to Third-Parties; and

5.2.4. such Data Subject(s) have not objected to the Processing of their Personal Data or requested the restriction of the Processing of their Personal Data.

5.3. Where the Data Controller is no longer lawfully entitled to Process any Personal Data it must notify the Data Processor immediately and request that the Data Processor ceases Processing such Personal Data. Furthermore, the Data Controller indemnifies the Data Processor against all Data Subject(s) and Third-Party claims and actions related to the unlawful Processing of Personal Data in providing the Services to the Data Controller.

6. DATA DELETION AND DE-IDENTIFICATION

6.1. Where the Data Processor is Processing Personal Data provided by the Data Controller, the Data Processor shall be entitled, from time to time, to Process the Data for archiving, data governance or information security related purposes.

6.2. Upon termination of the Agreement and subject thereto, or where instructed by the Data Controller (for example, in the case that a Data Subject has requested the erasure of any Personal Data), the Data Processor shall, at the instruction of the Data Controller, delete, de-identify, or return to the Data Controller all Data that it Processes on behalf of the Data Controller. If the Data Processor deletes any Personal Data permanently, such Personal Data may not be recovered.

6.3. Notwithstanding the above, and to the extent authorised or required by applicable law, the Data Processor may also retain one copy of the Personal Data for lawful business purposes or evidentiary purposes and/or for the establishment, exercise or defense of legal claims and/or for compliance with legal obligations.

7. DATA SUB-PROCESSORS / THIRD-PARTY DATA PROCESSORS

7.1. Under this Agreement, the Data Controller authorises the Data Processor to engage and utilise the services of other Third-Parties, within the scope and purposes of Processing the Data, including in particular, in order to provide the Software and related technical / service support.

7.2. A list of Third-Parties currently used by the Data Processor are included in Annexure 2 **"**Processing Instruction". The Data Controller authorises the Data Processor to engage these Third-Parties (as well as any other Third-Parties that it may require from time to time) as further Data Processors in order to provide the Services.

7.3. If the Data Processor engages a Third-Party Data Processor for carrying out specific Processing activities on behalf of the Data Controller, equivalent data protection obligations as set out in this Agreement will, where possible and where not already provided for by such Third-Party

Data Processor, be imposed on that Third-Party Data Processor, including in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the applicable Data Protection Laws.

8. CROSS-BORDER DATA TRANSFERS.

8.1. The Data Processor may, in delivering the Services, be required to transfer Data outside of the jurisdiction of the applicable Data Protection Laws and in such cases, the Data Controller represents and warrants that it has obtained adequate consents from applicable Data Subjects and, where required, any approval of a Data Protection Regulator. In any event the Data Controller warrants that it has a lawful basis on which to transfer the Data for such transfers. the Data Controller hereby authorises such transfers.

8.2. Where the Data is required to be transferred as such, the Parties shall ensure that the Personal Data are adequately protected and shall ensure that the recipients of such Personal Data are subject to appropriate contractual undertakings to ensure the confidentiality, non-disclosure and security of any Personal Data transferred to any Third-Party Data Processors.

9. SECURITY MEASURES & NOTIFICATIONS OF SECURITY COMPROMISES

9.1. The Data Controller shall ensure that adequate and appropriate security safeguards are established. These security safeguards are contained in Annexure 4 (Security Safeguards).

9.2. Should the Data Controller not mandate minimum security safeguards in Annexure 4, the Data Processor shall apply its own security safeguards.

9.3. Such security safeguards shall take appropriate, reasonable, technical and organisational measures to ensure that the integrity of the Personal Data in it's the Data Controllers possession or under its control is secure and that such Personal Data is protected against unauthorised processing, loss, unlawful destruction, damage or access by:

9.3.1. identifying reasonably foreseeable internal and external risks to Personal Data in its possession or under its control;

9.3.2. establishing and maintaining appropriate safeguards against the risks identified;

9.3.3. regularly verifying that the safeguards are effectively implemented; and

9.3.4. ensuring that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards; and

9.3.5. observing 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.

9.4. **Data Controller Notifications**:

9.4.1. Where there are reasonable grounds to believe that a security compromise has occurred on the systems of the Data Controller, the Data Controller shall notify the relevant Data Protection Regulator established under the Data Protection Laws.

9.4.2. The Data Controller must also notify the Data Processor of the Security Compromise, within 48 hours after discovery thereof, where there are reasonable grounds to believe that there has been any unauthorised access or acquisition of Personal Data on the Software, so as to enable the Data Processor to assess the security of the Software and where applicable, comply with its notification obligations under the Data Protection Laws.

9.5. **Data Processor Notifications**:

9.5.1. Where there are reasonable grounds to believe that a Security Compromise has occurred on the systems of the Data Processor, the Data Processor shall notify the Data Protection Commission and the data subject of the unauthorised access or acquisition, as soon as reasonably practicable, in accordance with the Data Protection Laws.

9.6. Where a Security Compromise occurs, the Data Controller shall take steps to ensure the restoration of the integrity of the information system.

10. LIABILITY

10.1. If either Party breaches any obligations under this Agreement or applicable Data Protection Laws, that Party shall be liable to the other Party and / or Data Subjects for (a) damages, losses, costs, taxes and expenses (including legal and professional fees); and (b) fines or penalties payable to the Data Protection Commission.

10.2. Such liability, in aggregate, shall not exceed the total Service fees paid by the by the Data Controller to the Data Processor.

10.3. The Parties agree and acknowledge that any damages, losses, costs, taxes and expenses (including legal fees) and regulatory fines incurred as a result of negligence, fault, gross negligence or misconduct shall be borne by the breaching Party and the other Party shall be indemnified by the breaching Party to that effect.

10.4. The Parties agree that any breach of any provision of this Agreement or applicable Data Protection Laws by the one of the Parties shall constitute a breach of the Agreement, entitling the other Party to terminate the Agreement in accordance with the provisions of the Agreement, notwithstanding any other rights it may have in Law.

11. COOPERATION ON DATA PROTECTION AND EXECUTION OF DATA SUBJECTS' RIGHTS

11.1. During the term of the Agreement, the Data Processor will assist the Data Controller (where reasonably possible) with its obligations to respond to Data Subject requests to access, rectify and/or restrict the Processing of the Data, including deletion of the Data.

11.2. The Data Processor will promptly notify the Data Controller if it receives a request from a Data Subject under any Data Protection Law in respect of the Data. The Data Controller will be responsible for responding to such requests, including any obligation to respond to requests for exercising Data Subject rights set out in the applicable Data Protection Law.

12. GOVERNING LAW AND JURISDICTION

12.1. With the exception to the relevant Data Protection Law, this Agreement is governed by the laws of the Republic of Ghana.

12.2. Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Ghana.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

KPI Lens Pty Ltd

(Duly authorised)

Signature ________________________________

Name: __________________________________

Title: ___________________________________

Date Signed: _____________________________

____

(Duly authorised)

Signature ________________________________

Name ________________________________

Title _________________________________

Date Signed ___________________________

13. ANNEXURE 1: DATA PROTECTION LAW

Where the Data Controller does not complete Annexure 1 or is based in a country without Data Protection Laws, the Data Processor shall implement the provisions of the Data Protection Act, 2012 of the Republic of Ghana.

The Data Controller is bound by the Data Protection Laws of________________________________.

The Data Protection Law defines Personal Data as:

____

____

____

The Data Protection Law defines Processing as:

____

____

____

Lawful basis for processing:

____

____

____

14. ANNEXURE 2: PROCESSING INSTRUCTION

14.1. The Data Controller requires the Data Processor to Process Personal Data of the following categories of Data Subjects:

____

____

____

____

14.2. The Data Controller is instructing the Data Processor to process the following categories of Personal Data:

____

____

____

____

14.3. The Data Controller requires the Data Processor to Process Personal Data to benefit from the Services. In particular, the Data Controller has the following specific purposes for Processing Personal Data

____

____

____

____

14.4. The Data Processor requires the services of the following Third Parties who will be sub-processors:

____

____

____

____

15. ANNEXURE 4: SECURITY SAFEGUARDS

This Annexure is to be read with Annexure 3 (Processing Instruction).
This Annexure shall only be signed and enforceable where the Data Processor is requested to implement security measures by the Data Controller.

Both Parties have implemented security safeguards relevant to the protection of Personal Data held by the Parties respectively.

In Particular the Data Controller warrants that it has given to 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 applicable in the Data Protection Laws.

The Data Processor acknowledges and accepts to be bound by the following specific security safeguards designed by the Data Controller:
Organisational:

____
____
____
____
____

Technical:

____
____
____
____
____

The Data Processor undertakes to inform the Data Controller as soon as reasonably practicable where any of the above security safeguards of compromised.

The Data Processor additionally undertakes to inform the Data Controller as soon as reasonably practicable where it has reason to believe that any Personal Data processed by the Data Processor on behalf of the Data Controller has been compromised, deleted, damaged or unlawfully accessed.

Such notifications shall be made in writing to a nominated representative of the Data Controller.
Signed for and on behalf of the Data Controller: _________________________

Signed for and on behalf of the Data Processor: _________________________