Idently Systems Limited

Data Processing Addendum

(Revised 28 April 2021)

This Data Processing Addendum ("DPA") is made between **Idently Systems Limited** a Kenyan company located at Four Greenway (2nd Floor), Westlands Road, Nairobi, Kenya (herein called "**Idently**") and Customer acting on its own behalf and as agent for each Customer Affiliate and forms part of the Original Agreement from the Effective date of the Original Agreement.

WHEREAS:

(A) Idently or a Idently Affiliate has entered into a certain agreement with Customer or a Customer Affiliate (the "Original Agreement") for the provision of products or services by Idently or a Idently Affiliate to or on behalf of Customer or a Customer Affiliate (the "Services") as further detailed in the Original Agreement.

(B) The parties agree that pursuant to the Services, Idently and/or a Idently Affiliate might receive or have access to certain Personal Data held by and controlled by Customer or a Customer Affiliate.

(C) The parties wish to be compliant with the Data Protection Laws, hence establish this DPA to describe the terms and conditions for the Processing activities in the context of the Services.

NOW THEREFORE, the parties agree as follows:

1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below:

1.1.1 "**Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with another entity , where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.2 **"Customer Group Member"** means Customer or any Customer Affiliate;

1.1.3 "**Customer Personal Data**" means any Personal Data Processed by Idently on behalf of Customer in connection with the Original Agreement;

1.1.4 "**Data Protection Laws**" means Kenya Data Protection Act 2019, as amended, replaced or superseded from time to time, including, but not limited to, any applicable Kenya laws and regulations relating to the Processing of Personal Data and privacy;

1.1.5 **"Idently Group Member"** means Idently or a Idently Affiliate;

1.1.6 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 1, amended as indicated in that Annex;

1.1.7 "**Subprocessor**" means any person (including any third party and any Idently Group Member, but excluding an employee of Idently or any of its sub-contractors) appointed by or on behalf of Idently to Process Customer Personal Data on behalf of any Customer Group Member in connection with the Original Agreement; and

1.1.8 "**Transfer**" means:

(i) a transfer of Customer Personal Data from Customer or Customer Group Member to Idently; or

(ii) an onward transfer of Customer Personal Data from Idently to a Subprocessor,

in each case, where such transfer would be prohibited by the Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of the Data Protection Laws) in the absence of appropriate safeguards as set out in clauses 3.5.2 and 8 below.

1.2 The terms, "**applicable data protection laws**", "**Commission**", "**Controller**", "**Data Subject**", "**Country**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", **"Processor"** and "**Supervisory Authority**" shall have the same meaning as in the Data Protection Laws.

2. Processing of Customer Personal Data

2.1 The parties agree that in respect of any Customer Personal Data processed in connection with the Original Agreement the Customer shall be the Controller and Idently shall be the Processor.

2.2 Idently shall process the Customer Personal Data only to the extent, and in such a manner, as is necessary for the purposes of the Original Agreement and in accordance with the Customer's lawful written instructions as set out in this DPA, including its Annexes and Appendices unless Processing is required by applicable laws to which Idently is subject. Idently must promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Laws.

2.3 The Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under Data Protection Laws.

2.4 Customer instructs Idently (and authorises Idently to instruct each Subprocessor) to Process Customer Personal Data and, in particular, transfer Customer Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the terms of the Original Agreement and this DPA.

3. Subprocessing

3.1 Customer authorises Idently to appoint Subprocessors in accordance with this clause 3 and any restrictions in the Original Agreement.

3.2 To the extent that any Subprocessor appointed by Idently processes Customer Personal Data then, Idently will remain responsible to the Customer for the Subprocessor's obligations under this DPA.

3.3 Idently may continue to use those Subprocessors already engaged by Idently as at the date of this DPA as identified in the Subprocessor list which can be accessed on Idently's Legal Repository webpage at https://www.Idently.com/repository/Idently-Subprocessors.pdf. For the avoidance of doubt, Customer specifically authorises the engagement of Idently Affiliates as Subprocessors.

3.4 Idently shall give Customer prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor by updating the Subprocessor list which is available in the Idently Legal Repository. If, within ten (10) days of receipt of that notice via the mechanism set out in this clause 3.3, Customer notifies Idently in writing of any objections (on reasonable grounds) to the proposed appointment Idently shall not appoint (or disclose any Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken. If the objection cannot be resolved by the parties within thirty (30) days of receipt by Idently of the objection, Idently shall not be in breach of the Original Agreement to the extent that it cannot provide the Services or otherwise comply with its obligations as a result.

3.5 With respect to each Subprocessor, Idently shall:

3.5.1 ensure that the arrangement between (a) Idently, or (b) the relevant Idently Affiliate; and the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA, in particular in relation to requiring the Subprocessor to implement appropriate technical and organizational measures, and meet the requirements of the Data Protection Laws;

3.5.2 if that arrangement involves a Transfer, ensure that appropriate safeguards as set out in clause 8.1.1 and clause 8.1.2 are at all relevant times in place between (a) Idently, or (b) the relevant Idently Affiliate; and the Subprocessor; and

3.5.3 provide to Customer for review such copies of the Idently or Idently Affiliate's agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this DPA) as Customer may request from time to time.

3.6 Idently shall ensure that each Subprocessor performs the obligations under clauses 2.2, 6.1, and 7.2, as they apply to Processing of Customer Personal Data carried out by that Subprocessor, as if it were party to this DPA in place of Idently.

4. Idently's personnel

4.1 Idently shall ensure that its personnel engaged in the Processing of Customer Personal Data are informed of the confidential nature of the Customer Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

4.2 Idently shall ensure that access to Customer Personal Data is limited to those personnel who require such access to perform the Services.

5. Security

5.1 Idently will implement appropriate technical and organizational measures against unAuthorized or unlawful Processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Customer Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Customer Personal Data as set out in Appendix 2.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Idently shall assist each Customer Group Member by implementing the technical and organizational measures set forth in Appendix 2, insofar as this is possible, for the fulfilment of the Customer Group Members' obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws. Idently and Customer acknowledge that they consider these measures to be appropriate, taking into account the nature of the Processing.

6.2 Idently shall:

6.2.1 promptly notify Customer if any Idently Group Member receives a request from a Data Subject under any Data Protection Laws in respect of Customer Personal Data; and

6.2.2 ensure that the Idently Group Member does not respond to that request except on the instructions of Customer or the relevant Customer Affiliate or as required by applicable laws to which the Idently Group Member is subject, in which case Idently shall to the extent permitted by applicable laws inform Customer of that legal requirement before the Idently Group Member responds to the request.

7. Personal Data Breach

7.1 Idently shall notify Customer without undue delay upon any Idently Group Member becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or the relevant Supervisory Authority of the Personal Data Breach under the Data Protection Laws.

7.2 Idently shall co-operate with Customer and take such reasonable commercial steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Cross-border transfers of Customer Personal Data

8.1 Idently may only process, or permit the Processing, of Customer Personal Data outside Kenya under the following conditions:

8.1.1 Idently is Processing Customer Personal Data in a territory that provides adequate protection for the privacy rights of individuals; or

8.1.2 Idently and the Customer have executed the Standard Contractual Clauses in Annex 1 (unless the parties agree another more appropriate lawful data transfer mechanism exists).

9. Deletion or return of Customer Personal Data

9.1 Subject to clause 9.2 Idently shall promptly and in any event within thirty (30) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), delete and procure the deletion of all copies of the Customer Personal Data, unless applicable law or regulation requires its storage.

9.2 Subject to clause 9.1, Customer may by written notice to Idently within ten (10) days of the Cessation Date require Idently to (a) return a copy of all Customer Personal Data to Customer in a mutually agreeable format; and (b) delete and procure the deletion of all other copies of Customer Personal Data Processed by any Idently Group Member. Idently shall comply with any such written request within thirty (30) days of the Cessation Date.

9.3 Idently shall provide written certification to Customer that it and each Idently Affiliate has fully complied with this clause 9 upon Customer's written request.

10. Audit Rights, Assistance and Privacy Impact Assessments

10.1 The parties agree that the audits described in clause 5(f) and clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

10.1.1 Idently shall, in accordance with the Data Protection Laws, make available to the Customer such information in Idently's possession or control as the Customer may reasonably request with a view to demonstrating Idently's compliance with the obligations of a Processor under the Data Protection Laws in relation to its Processing of Customer Personal Data.

10.1.2 The Customer may exercise its right of audit under the Data Protection Laws in relation to Customer Personal Data, through Idently providing:

(i) an audit report not older than eighteen (18) months, prepared by an independent external auditor demonstrating that Idently's technical and

organizational measures are sufficient and in accordance with an accepted industry audit standard; and

(ii) additional information in Idently's possession or control to a Kenyan Supervisory Authority when it requests or requires additional information in relation to the Processing of Customer Personal Data carried out by Idently under this DPA.

10.1.3 Idently will provide reasonable assistance to respond to Customer's questions concerning the Services (provided Customer will pay Idently's reasonable costs) to enable Customer to assess and consider reasonable mitigation measures when carrying out a data protection impact assessment.

10.1.4 If Customer requires additional information, assistance or audit to demonstrate Idently's compliance with its obligations under this DPA, then Idently will provide reasonable information and assistance on at least thirty (30) days' notice (unless Customer can demonstrate that the request is urgent), provided the Customer pays Idently's reasonable costs.

11. Term

11.1 This DPA shall remain in full force and effect so long as the Original Agreement remains in effect or a Idently Group Member retains any Personal Data relating to the Original Agreement in its possession or control.

12. Notice

12.1 Any required notice to be given under or in connection with this DPA shall be in writing and sent by first class post or by email to:

12.1.1 in the case of Idently: DPO@Idently.com;

12.1.2 in the case of Customer: the contact details detailed in the Original Agreement.

13. General Terms

Entire Agreement

13.1 This DPA including its Annexes and referenced documents together with the Original Agreement constitutes the entire agreement between the parties as it relates to the Processing of Customer Personal Data and supersedes any previous agreements, arrangements, undertakings or proposals, written or oral, between the parties in relation to its subject matter.

Governing law and jurisdiction

13.2 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.2.1 the parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Original Agreement with respect to any disputes or claims howsoever arising

under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.2.2 this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Original Agreement.

Order of precedence

13.3 Nothing in this DPA reduces Idently's obligations under the Original Agreement in relation to the protection of Customer Personal Data or permits Idently to Process (or permit the Processing of) Customer Personal Data in a manner which is prohibited by the Original Agreement. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.4 Subject to clause 13.3, with regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Original Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

Severability

13.5 Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

No variation

13.6 No modification or variation of this DPA (or any document entered into pursuant to or in connection with the DPA) shall be valid unless it is in writing and signed by or on behalf of each of the parties to this DPA.

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Original Agreement with effect from the Effective Date.

Customer

Signature: _____

Name: _____

Title: _____

Date Signed: _____

Idently Systems Limited:

Signature: _____

Name: George Mukenya

Title: CEO

Date Signed:

ANNEX 1

STANDARD CONTRACTUAL CLAUSES

For the purposes of the Kenya Data Protection Act, 2019, for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization:

Address:

Tel.:_____; fax:_____; e-mail: _____

Other information needed to identify the organization

……

(the data **exporter**)

And

Name of the data importing organization: **Idently Systems Limited**

Address: Four Greenway (2nd Floor), Westlands Road, Nairobi, Kenya

Tel.: +254 734467635 e-mail: dpo@Idently.com

Other information needed to identify the organization: Not applicable

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a Data Processing Addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that Services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with the Kenya Data Protection Act, 2019 and applicable data protection laws, the data exporter agrees to the provision of such Services, including

the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in the Kenya Data Protection Act, 2019 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of the Kenya Data Protection Act, 2019;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Country in which the data exporter is established;

(f) *'technical and organizational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unAuthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 of the DPA which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Country where the data exporter is established) and does not violate the relevant provisions of that Country;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unAuthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful

forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of the Data Protection Laws;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unAuthorized access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise Authorized to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Arbitration and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to arbitration, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Country in which the data importer is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Country in which the data importer is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Country in which the data importer is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature…….

On behalf of the data importer:

Name (written out in full): George Mukenya
Position: CEO
Address: Four Greenway (2nd Floor), Westlands Road, Nairobi, Kenya
Other information necessary in order for the contract to be binding (if any): None

Signature…….

APPENDIX 1 TO THE DPA AND STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Data exporter
Where applicable, the data exporter is: Customer

Data importer
Where applicable, the data importer is: Idently Systems Limited

Data subjects
The personal data transferred concern the following categories of data subjects:

- Prospects, customers, business partners and vendors of data exporter (who are natural persons)
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors
- Employees, agents, advisors, consultants, or contractors of data exporter
- Data exporter's users authorized to use the Services

Categories of data
The personal data transferred concern the following categories of data:

Identification data
Personal Identification Data such as name, title, address (private, work), former addresses, telephone number (private, work).
Identification details issued by the government such as ID number, passport number, driver license number.
Electronic identification data such as accounts, mail address, IP addresses.

Financial data
Financial identification data such as bank account numbers, credit or debit card numbers.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
None

Processing operations
The personal data transferred will be subject to the following basic processing activities:

In support of the services and other activities to be supplied to or carried out by or on behalf of Idently for Customer pursuant to the Original Agreement

DATA EXPORTER

Name:……
Authorized Signature ……

DATA IMPORTER

Name: George Mukenya, CEO
Authorized Signature ……..……

APPENDIX 2 TO THE DPA AND STANDARD CONTRACTUAL CLAUSES

Where applicable, this Appendix forms part of the Clauses and must be completed and signed by the parties.

The Data Importer currently abides by the security standards in this Appendix 2. The Data Importer may update or modify these security standards from time to time provided such updates and modifications will not result in a material decrease of the overall security of the Services during the term of the Original Agreement.

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. The bodies of policy management

For the its operation as a Certification Authority, Idently employs two internal teams that manage policies within the company: one is the Policy Authority and the other is the Data Protection Office.

(a) Policy Authority
The Policy Authority consists of various committees focusing on specific areas that focus on strategizing, defining and managing policies and procedures, and flow those decisions down to departmental heads for implementation. Policy Authorities 3.1 - 3.10 are sub authorities that manage policies related to security, such as Information Security Policy and Principles, Physical Security Policy, Logical Security Policy, Personnel Security Policy, Third Party Management Policy, Secure Development, Change Management Policy, and Business Continuity Management policy. All of the security measures described below are implemented based on these policies.

(b) Data Protection Office
Idently also maintains a task force called the Data Protection Working Group (DPWG) under the direction of the Data Protection Officer who is appointed by the Idently CEO and has the delegated authority for enforcing Idently personal data processing and transfer related policies.

2. Data Center & Network Security.

(a) Data Centers.

Infrastructure. Idently maintains its systems in geographically distributed data centers in Nairobi (Kenya) and Mombasa (Kenya), and stores all production data in a secure environment with strong physical access barriers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks, power systems or other necessary devices help provide this redundancy. In the event of a power outage, backup power is provided by UPS batteries and diesel generators to provide enough electrical power typically for a period of days.

Server Operating Systems. Idently servers use a Linux based implementation customized for the application environment to augment data security and redundancy. Idently employs a code

review process to increase the security of the code used to provide the services and enhance the security products in production environments.

Businesses Continuity. Idently replicates data over multiple servers across different geographical regions, and uploads encrypted data to cloud storage daily as backup to protect against accidental destruction or loss. Idently has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks & Transmission

Internal Networks. All the internal networks, i.e. Idently intranet, are strictly isolated by firewalls from external networks to prevent unauthorized access.

Data Transmission. Data transmission between Idently offices and the data centers is typically connected via high-speed private links, i.e. VPN (IPSEC with AES256), to provide secure data transfer between data centers and offices so that data can't be read, copied, altered without authorization during transfer within Idently.

In addition to the above environment, the Certificate Management Protocol (CMP) is implemented between RA systems and CA systems to maintain the highest security level of industry standard.

External Attack Surface. Idently employs multiple layer networks and strong filtering controls for external facing systems. Recurring vulnerability assessment (quarterly) and penetration testing exercises (annually) are conducted in addition to any in the case of significant changes to the systems.

Intrusion Detection. Idently employs intrusion detection and prevention systems on both our office and data center networks. Idently intrusion detection involves:

1. Employing intrusion detection, 24 X 7 monitoring service by security professionals who are tightly integrated with the Idently incident response team; and
2. Employing technologies that automatically remedy certain potentially dangerous situations.

Incident Response. Idently maintains security personnel, i.e. the incident response team, who monitor a variety of communication channels for security incidents, including the notification of events from intrusion detection system (IDS) professionals, and react promptly in the event of any incident.

Encryption Technologies. Idently makes HTTPS encryption (RSA2048) available, as well as IPSEC for interoffice communications with AES256.

(c) Idently Intranet

Managed Devices. To connect to the LAN segment of the Idently intranet, the device must have a digital certificate issued by Idently's IT department.

Active Directory. Idently employs central authentication mechanisms, i.e. Active Directory, before access to the Idently intranet resources is permitted.

Login procedures/ authentication mechanism. To access intranet resources within Idently, at least the following steps must be performed correctly:

- Boot up Idently managed PC
- Device authentication via digital certificate
  (PKI authentication protocol shall be performed for the device certificate)
- Insert IC-card ID, issued for individuals, and activate the IC- Card by entering password (long and strong password, mandatory combination of alpha/numeric/symbols)
- Login to AD by entering AD password (password, different from IC-Card password)
  (PKI authentication protocol shall be performed for individual certificate)
- Dual (OTP) authentication for each individual service.

Other countermeasures. To minimize the risks of malware attacks only members of the IT department have administrator privileges. Segregation of duties and other industry standard practices are in place as specified in Idently internal policies.

3. Access and Site Control

(a) Site Controls

On-site Data Center Security Operation. Idently maintains an on-site security operation responsible for all physical data center security functions 24 X 7. The on-site security operation personnel monitor CCTV cameras and all alarm systems.

Data Center Access Procedures. Idently maintains formal access procedures for allowing physical access to the data centers. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security.

All other entrants requiring temporary data center access must: (i) obtain approval in advance for the specific data center; (ii) sign in at on-site security operations; and (iii) must be accompanied by Idently authorized employees at all times.

On-site Data Center Security Devices. Idently's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate.

(b) Access Control

Infrastructure Security Personnel. Idently maintains a security policy for its personnel and requires specific security training as part of the training package for these personnel. Idently's infrastructure security personnel are responsible for the ongoing monitoring of the security infrastructure, the review of the services, and responding to security incidents.

Access Control and Privilege Management. The Idently Certification Center (ICC) account's administrators must authenticate themselves via ICC systems in order to administer the services.

Internal Data Access Processes and Policies – Access Policy. Idently's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Idently designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording.

4. Data Access and Site Control

(a) Data Storage, Isolation & Logging

Idently stores data in a multi-tenant environment on Idently-owned servers, as well as cloud service providers. The data and file system architectures are replicated between multiple servers. Idently employs central logging server in data centers, typically isolated from application servers.

(b) Decommissioned Disks and Disk Erase Policy
Decommissioned disks are erased in a multi-step process, and recorded according to Idently policies, i.e. Idently Retention Policy and internal disposal and destruction standards.

5. Personnel Security

Idently personnel are required to conduct themselves in a manner consistent with the Idently user guidelines and other policies regarding confidentiality, appropriate usage, and professional standards.

Idently conducts appropriate backgrounds checks for the personnel who deal with critical operations, i.e. Trusted Roles, to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Idently's confidentiality and privacy policies.

6. Subprocessor Security

Prior to onboarding Subprocessors, Idently conducts security self-check questionnaires of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged.

Once Idently has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms, as described in the addendum of Idently to ensure compliance with the obligations of article 28 of the General Data Privacy Regulation.

7. Data Protection Office

The Data Protection Office of Idently can be contacted at: dpo@Idently.com via e-mails (or other means as provided in the Idently Privacy Policy).

DATA EXPORTER

Name:……
Authorized Signature ……

DATA IMPORTER

Name: George Mukenya, CEO
Authorized Signature ……