HEL

HERITAGE ECOLOGICAL LIMITED

Heritage Ecological Ltd

UK GDPR - Data Processing Agreement

January 2022

UK GDPR Data Processing Agreement between a Controller and a Processor (for use within the UK)

****This document should be completed after reading our Guidance Notes on completing the Data Processing Agreement between a Controller and a Processor]**

This agreement is made on [DAY] of [YEAR]

Parties to this agreement:

(1) [FULL COMPANY NAME] incorporated and registered in [ENGLAND AND WALES] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (the "Controller");

and

(2) [FULL COMPANY NAME] incorporated and registered in [ENGLAND AND WALES] with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (the "Processor").

Background and Scope

(A) The Controller determines the purposes and means of processing Personal Data in connection with its business activities;

(B) The Processor processes Personal Data on behalf of the Controller;

(C) The Controller wishes to engage the services of the Processor to process personal data on its behalf;

(D) The UK GDPR provides that, where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the UK GDPR and ensure the protection of the rights of the data subject;

(E) The UK GDPR further provides that the Processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes;

(F) The UK GDPR further provides that, the Processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by law;

(G) In compliance with the above-mentioned provisions of the UK GDPR the Controller and Processor wish to enter into this processing agreement.

The parties hereby mutually agree the following:

1. Definitions and Interpretation

1.1 In this agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"Appendix 1" means the appendix to this agreement and which forms part of this agreement;

"UK GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act of 2018;

"**Controller, data controller, processor, data processor, data subject, personal data, special categories of personal data, personal data breach, supervisory authority, processing and appropriate technical and organisational measures"**: as set out in the Data Protection Legislation in force at the time;

"Confidential Information" means all information disclosed by a party to the other party pursuant to this agreement which is either designated as proprietary and/or confidential, or by its nature or the nature of the circumstances surrounding disclosure, should reasonably be understood to be confidential, including (but not limited to), information on products, customer lists, price lists and financial information;

"Data Protection Legislation": means the data protection and privacy legislation which is in force in the UK and it includes the Data Protection Act 2018, the UK GDPR and the Privacy and Electronic Communications Regulations 2003;

"Services" means [PLEASE DESCRIBE THE SERVICE]. The Services is described more in detail in Appendix 1;

"Sub-contract" and "sub-contracting" shall mean the process by which either party arranges for a third party to carry out its obligations under this agreement;

"Sub-processor" means the party to whom the obligations are sub-contracted.

2. Consideration

2.1 In consideration of the Controller engaging the services of the Processor to process personal data on its behalf, the Processor shall comply with the security, confidentiality and other obligations imposed on it under this agreement and any applicable Data Protection Legislation.

3. Processing Details

3.1 The Controller hereby confirms the processing details:

Subject matter of the processing	[INSERT DETAILS]
The duration of the processing	[INSERT DETAILS]
The nature of the processing	[INSERT DETAILS]
The type of personal data being handled	[INSERT DETAILS]
The purpose of the processing	[INSERT DETAILS]
The categories of data subjects to whom the personal data relates	[INSERT DETAILS]
The obligations and rights of the data controller	[INSERT DETAILS]

3.2 Without prejudice to the generality of clause 5.2, the Controller will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Processor for the duration and purposes of this agreement.

4. A) Obligations of the Processor

The Processor agrees to:

4.1 Process the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 Take into account the nature of the processing, and to assist the Controller through appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in the Data Protection Legislation. In addition the Processor shall:

4.2.1 Promptly notify the Controller if it receives a request from a Data Subject under any Data Protection Legislation in respect of Controller Personal Data; and

4.2.2 Ensure that the Processor does not respond to that request except on the documented instructions of Controller or as required by Data Protection Legislation to which the Processor is subject, in which case the Processor shall, to the extent permitted by Data Protection Legislation, inform the Controller of that legal requirement before the Processor responds to the request.

4.3 Take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

4.4 Take account in assessing the appropriate level of security the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

4.5 Have in place appropriate technical and organisational security measures, reviewed and approved by the Controller, to protect the personal data provided or made available by the Controller to the Processor in the context of this agreement, as required under the Data Protection Legislation. Further details, including the minimum standard of security protection, are set out in Appendix 1 of this agreement.

4.6 For the avoidance of doubt, nothing within this agreement relieves the Processor of its own direct responsibilities and liabilities under the UK GDPR.

4. B) Additional Obligations of the Processor

The Processor further agrees, by taking into account the nature of processing and the information available to the Processor, to:

4.7 Assist the Controller in meeting obligation to keep personal data secure;

4.8 Assist the Controller in meeting its obligation to notify personal data breaches to the supervisory authority, this includes:

4.8.1 Notifying the Controller without undue delay upon the Processor or any Sub-processor becoming aware of a Personal Data Breach affecting Controller Personal Data.

4.8.2 Such notification shall as a minimum:

a) Describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;
b) Communicate the name and contact details of Processor's data protection officer or other relevant contact from whom more information may be obtained;
c) Describe the likely consequences of the Personal Data Breach; and
d) Describe the measures taken or proposed to be taken to address the Personal Data Breach.

4.8.3 In addition, to co-operate with the Controller and to take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

4.9 Assist the Controller in meeting its obligation to advise data subjects when there has been a personal data breach;

4.10 Assist the Controller in meeting its obligation to carry out data protection impact assessments (DPIAs); and

4.11 Assist the Controller in meeting its obligation to consult with the supervisory authority where a DPIA indicates there is an unmitigated high risk to the processing.

5. Other Obligations for Both Parties

5.1 The Controller and Processor shall take steps to ensure that any natural person acting under the authority of the Controller or the processor who has access to personal data does not process them except on instructions from the Controller, unless he or she is required to do so by law.

5.2 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause 5.2 is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.

6. Confidentiality

6.1 The Processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

6.2 In particular, the Processor agrees that, save with the prior written authorisation of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

6.3 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller and as agreed in this agreement.

6.4 The obligations in clauses 6.1, 6.2 and 6.3 above shall continue for a period of [FIVE] years after the cessation of the provision of services by the Processor to the Controller.

6.5 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

7. Engaging another processor

7.1 The Processor shall not engage another processor without the prior specific or general written authorisation of the Controller.

7.2 In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Controller the opportunity to object to such change and to terminate the agreement as a result of this change.

7.3 Where the Processor, with the authorisation of the Controller, engages another processor for carrying out its obligations under this agreement or other legal act, it shall do so only by way of a written agreement with the Sub-processor which imposes at least the same level of protection for the Controller as set out in this agreement or other legal act, including but not limited to providing sufficient guarantees in relation to the security of the processing on the Sub-processor as are imposed on the Processor under this agreement.

7.4 The Processor agrees to provide to the Controller for review such copies of the written agreement between the Processor and the Sub-processor (which may be redacted to remove confidential commercial information not relevant to the requirements of this agreement) as the Controller may request from time to time.

7.5 For the avoidance of doubt, where the Sub-processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the fulfilment of that other processor’s obligations.

8. Price and payment

8.1 The Controller shall pay the Processor for the Services the amounts described in Appendix 1.

8.2 Any amount mentioned in this agreement shall be VAT exclusive.

8.3 Invoices shall be paid within a period of thirty [30] days following receipt thereof.

9. Audits and Inspections

The Processor agrees to:

9.1 Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this agreement and the Data Protection Legislation;

9.2 Allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

9.3 The Processor shall immediately inform the Controller if, in its opinion, an instruction pursuant to this section 9 infringes the Data Protection Legislation.

10. Term and Termination

10.1 This agreement shall continue in full force and effect for [INSERT DETAILS FOR EXAMPLE ONE (1) YEAR] FROM THE DATE OF SIGNATURE OF THIS AGREEMENT].

10.2 Either Party shall have the right to terminate the Agreement, partially or entirely, forthwith by sending a written notice of termination to the other Party specifying the reasons for the termination, if any of the following events occur:

10.2.1 The other party materially breaches any of its obligations under this agreement;

10.2.2 The other party breaches any of its obligations under this agreement and, notwithstanding a written request from the non-breaching party to remedy such a breach, fails to comply with such a request within a period of thirty [30] days following such notice;

10.2.3 An event of force majeure prevails for a period exceeding three (3) months; or

10.2.4 The other party becomes insolvent or enters liquidation, a petition in bankruptcy is filed for it or a receiver is appointed.

10.3 Upon the termination or expiry of this agreement, any rights and obligations of the parties, accrued prior to the termination or expiry thereof shall continue to exist.

10.4 Within [INSERT] days following termination of this agreement the Processor shall, at the direction of the Controller, either (a) return all personal data passed to the Processor by the Controller for processing, or (b) on receipt of instructions from the Controller, destroy all such data unless the Processor is prohibited from doing so by any applicable law.

10.5 The Processor may retain Controller Personal Data to the extent required by Data Protection Legislation and only to the extent and for such period as required by Data Protection Legislation and always provided that the Processor and any sub-processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only processed as necessary for the purpose(s) specified in the Data Protection Legislation requiring its storage and for no other purpose.

10.6 The Processor shall provide written certification to Controller that it and any sub-processor has fully complied with this section 10 within [INSERT DATE] of the termination date.

11. Intellectual Property Rights

11.1 The Processor is and shall remain the owner of any materials used or made available in the context of the delivery of the services.

11.2 The Processor grants to the Controller a limited, personal, non-exclusive, non-transferable right to use any material provided in the context of the delivery of the services. This license is valid for the duration of the agreement.

11.3 The Controller is and shall remain the owner of any personal data supplied or made available to the Processor in the context of this agreement.

11.4 The Controller grants to the Processor a limited, personal, non-exclusive, non-transferable right to use any personal data provided only in the context of the delivery of the services. This license is valid for the duration of the agreement.

12. Governing Law

12.1 This agreement shall be governed by and construed exclusively in accordance with the laws of England and Wales.

13. Entire agreement

13.1 This agreement contains the entire agreement and understanding between the parties with respect to the subject matter hereof and supersedes and replaces all prior agreements or understandings, whether written or oral, with respect to the same subject matter that are still in force between the parties.

13.2 Any amendments to this agreement, as well as any additions or deletions, must be agreed in writing by both the parties.

14. Severance

14.1 Should any provision of this agreement be invalid or unenforceable, then the remainder of this agreement 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.

AS WITNESS this agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [CONTROLLER]

…………………………………

(Authorised signatory)

…………………………………

(Print name and title)

SIGNED on behalf of [PROCESSOR]

…………………………………

(Authorised signatory)

…………………………………

(Print name and title)

APPENDIX 1:

1. Description of the services and pricing

[a. Please add a description of the Services]

[b. Please add a description of the Pricing/Invoicing model.]

2. Technical and Organisational Measures

2.1 In compliance with its obligations under clause 4 with regard to the processing of personal data on behalf of the Controller, the Processor, as a minimum requirement, shall implement appropriate technical and organisational measures to comply with the Data Protection Legislation. This includes the following requirements:

2.1.1 The pseudonymisation and encryption of personal data;

2.1.2 The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

2.1.3 The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

2.1.4 A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

This document is intended to serve as general guidance only and does not constitute legal advice. The application and impact of laws can vary widely based on the specific facts involved. This document should not be used as a substitute for consultation with professional legal or other competent advisers. Before making any decision or taking any action, you should consult a Markel Law professional.

In no circumstances will Markel Law LLP, or any company within the Markel Group be liable for any decision made or action taken in reliance on the information contained within this document or for any consequential, special or similar damages, even if advised of the possibility of such damages.