etiCloud Ltd
Enterprise House,
1 Broadfield Court
Sheffield S8 0XF
everythingthatis.cloud

etiCloud Ltd Data Processing Agreement for Customers
Private and Confidential

DATA PROCESSING TERMS

1 – Term and effect

1.1) This Agreement shall be deemed to have commenced on the Effective Date and shall continue in force unless and until such time as the Services Agreement expires or is terminated in accordance with its terms.
1.2) This Agreement shall take priority over any Services Agreement that the Customer has entered into with ETICLOUD for the provision of the Services to the extent of any conflict or inconsistency between any provision of this Agreement and the Services Agreement. For the avoidance of doubt, the terms and conditions of the Services Agreement relating to limitations and exclusions of liability, force majeure and other rights of relief set out for either Party's benefit in the Services Agreement shall also apply to this Agreement.

2 – Relationship of the Parties

2.1) The Parties agree that they may each process various types of Personal Data in relation to the performance and receipt of the Services and the Parties' respective business operations.
2.2) Each Party shall comply with its obligations under this Agreement and under Data Protection Law with respect to the types of Personal Data it processes and according to its responsibilities as a controller, processor or joint controller (as appropriate) for the relevant Personal Data, as described in the ETICLOUD Data Processing Schedule.

3 – Controller obligations

Whenever a Party is acting in a capacity as a controller in relation to Personal Data, it shall comply in all respects with Data Protection Law and shall:
a) process such data fairly and lawfully;
b) implement appropriate technical and organisational measures to protect such Personal Data against Data Security Incidents; and
c) provide all assistance reasonably required by the other Party in order for that other Party to comply with such obligations, including with respect to data subject access requests.

4 – Processor obligations

4.1) Where a Party (the "**Processor**") is processing Personal Data on behalf of the other Party, whether as a processor or sub-processor, and not as a controller or joint controller, the following provisions shall apply:
4.2) Purpose limitation
The Processor shall process the Personal Data as necessary: (i) to perform its obligations under this Agreement and under the Services Agreement; (ii) to comply with its obligations under Applicable Law; and (c) to enhance the Services (the "**Permitted Purpose**"), except where otherwise required by any Applicable Law. In no event shall the Processor process the Personal Data for its own purposes or those of any third party.

4.3) Documented instructions

The Processor shall process the Personal Data only on documented instructions from the other Party, which may include the instructions set out in this Agreement and the Services Agreement, and shall immediately inform the other Party if, in its opinion, an instruction infringes Data Protection Law.

4.4) Categories of Personal Data

The Parties agree that the categories of Personal Data that are processed in connection with this Agreement may include CRM Data, User Data, Communications Data and Content. The ETICLOUD Data Processing Schedule identifies when ETICLOUD processes such categories of Personal Data in the provision of services to its customers and whether ETICLOUD is acting as a Controller or Processor for the purposes of such processing. ETICLOUD may amend or update the ETICLOUD Data Processing Schedule from time to time by making available a revised version. In the event that ETICLOUD wishes to amend its responsibility as a Controller or Processor as set out in the ETICLOUD Data Processing Schedule or materially change the categories of Personal Data that ETICLOUD processes as a Processor in connection with the provision of the Services, ETICLOUD will endeavour to give the Customer at least 30 days' written notice of the change. Where ETICLOUD is acting as a Processor, it is the Customer's responsibility to determine if any further details of ETICLOUD's activities need to be recorded in this Agreement to comply with Data Protection Law and ETICLOUD shall act in good faith to cooperate with any reasonable request to do so. ETICLOUD would only update the Data Processing Schedule where legislation requires ETICLOUD to do so.

4.5) International transfers

The Processor shall not permit any Processing of Personal Data outside the UK unless:

a) the Processor first puts in place adequate transfer mechanisms to ensure the transfer is in compliance with Data Protection Law;

b) the Processor or the relevant Authorised Sub-Processor is required to transfer the Personal Data to comply with Applicable Law, in which case the Processor will notify the other Party of such legal requirement prior to such transfer unless such Applicable Law prohibits such notice from being given to the other Party; or

c) the Processor is entitled to rely on a permitted derogation under Data Protection Law in order to transfer the Personal Data outside of the UK, which may include circumstances where (among other things): (i) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (ii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; or (iii) the transfer is necessary for the establishment, exercise or defence of legal claims.

For the purposes of clause 4.5(a), the adequate transfer mechanisms may include: (i) transferring the Personal Data to a recipient in an Adequate Territory, (ii) transferring the Personal Data to a recipient that has achieved binding corporate rules authorisation in accordance with Data Protection Law, or (iii) transferring the Personal Data to a recipient that has executed Standard Data Protection Clauses with the Processor.

4.6) Confidentiality of processing
The Processor shall ensure that any person that it authorises to process the Personal Data (including the Processor's staff, agents and subcontractors) (each an "**Authorised Person**") shall be under an obligation (whether under contract or statute) to keep the Personal Data confidential.
4.7) Security
The Processor shall implement appropriate technical and organisational measures to protect the Personal Data from Data Security Incidents. Such measures shall have regard to 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. Where ETICLOUD is the Processor, it shall comply with its Security Policy.
4.8) Sub-processing
The Processor shall be authorised to engage third parties to process Personal Data on behalf of the other Party (as a controller), provided that it notifies the other Party of such engagement (each, an "**Authorised Sub-Processor**") thereby giving the other Party the opportunity to object to such changes. The Processor will ensure that there is in place a written contract between the Processor and the Authorised Sub-Processor that specifies the Authorised Sub-Processor's processing activities and imposes on the Authorised Sub- Processor equivalent terms as those imposed on the Processor in this clause 4. The Processor will remain responsible for the acts and omissions of Authorised Sub-Processors in respect of their processing of Personal Data as if they were its own. Where the Processor is instructed by the other Party to grant access to Personal Data to a third party who is contracted to the other Party (a "**Contracted Third Party**"), the Contracted Third Party shall not be a sub-processor of the Processor for the purposes of this clause 4.8 and the other Party shall have sole responsibility for putting in place an appropriate data processing agreement with the Contracted Third Party that complies with Data Protection Law.
4.9) Cooperation
The Processor shall:
a) taking into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising data subjects' rights;
b) assist the controller in implementing appropriate technical and organisational measures against Data Security Incidents, completing data protection impact assessments and notifying Data Security Incidents to the competent supervisory authority or to the data subjects concerned, as required by Data Protection Law and taking into account the nature of the processing and the information available to the Processor.
If compliance with this clause 4.9 requires: (i) a change to the Services performed by ETICLOUD, (ii) a change to the Services Agreement under which the relevant Services are provided, or (iii) the expenditure of material effort or cost that is not provided in the Services Agreement, then either ETICLOUD or the Customer may raise this in accordance with the change control procedure set out in the Services Agreement or, in the absence of any such change control procedure, by discussing the same in good faith. For the avoidance of doubt, ETICLOUD shall not be required to provide any assistance under this clause 4.9 that would result in any change or expenditure referred to in paragraph (i) to (iii) of this clause 4.9, except if and to the extent that a suitable change is agreed to the Services Agreement.
4.10) Data protection impact assessments
If the Processor believes or becomes aware that its processing of Personal Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform

the other Party and provide the other Party with assistance to conduct a data protection impact assessment in accordance with clause 4.9.

4.11) Data Security Incidents

a) Upon becoming aware of a Data Security Incident, the Processor shall inform the other Party without undue delay (and in any event within 48 hours) and shall provide such timely information and assistance in accordance with clause 4.9 as the other Party may require in order for the other Party to fulfil its data breach reporting obligations under Data Protection Law and to mitigate the effects of the Data Security Incident.

b) Where ETICLOUD is acting as the Processor, the Customer understands and accepts that the performance by ETICLOUD of certain Services may carry a risk to the Customer of loss or corruption of data. ETICLOUD's obligations in respect of data backup or retention shall be set out in the applicable Services Agreement. The Customer understands and accepts that, save to the extent of any obligations detailed in this Agreement or the relevant Services Agreement, the Customer shall bear full responsibility for the loss or corruption of data that may result from a Data Security Incident.

4.12) Subject access requests

The Processor shall promptly notify the other Party if it receives a request from a data subject to exercise their rights in respect of their Personal Data and shall provide such assistance to the other Party as may be required in accordance with clause 4.9.

4.13) Deletion or return of Personal Data

Upon termination or expiry of this Agreement, the Processor shall (at the other Party's election) destroy or return to the other Party all Personal Data (including all copies of the Personal Data) in its possession or control (including any Personal Data that is processed by an Authorised Sub-Processor). This requirement shall not apply to the extent that the Processor is required by any Applicable Law to retain some or all of the Personal Data, in which event the Processor shall isolate and protect the Personal Data from any further processing except to the extent required by such Applicable Law. The Processor shall be entitled to render such charges or recover such costs associated with destroying or returning Personal Data to the controller or joint controller (as appropriate) as provided in the Services Agreement or, if no such charges or costs are provided in the Services Agreement, such reasonable costs that the Processor can evidence.

4.14) Information and audit

The Processor shall make available to the other Party all information necessary to demonstrate compliance with the obligations set out in this clause 4 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, except if and to the extent that providing such information or permitting such an audit would place the Processor in breach of Applicable Law or cause it to infringe the rights (including rights in intellectual property or confidential information) of any of the Processor's other customers. No more than one audit may be carried out in any calendar year, except if and when required by instruction of a competent data protection authority. The Processor shall be entitled to recover its costs of complying with this clause 4.14. Where the Processor has appointed a third party auditor to assess any of its technical or organisational measures to protect against Data Security Incidents for the purposes of any industry certification or otherwise (such as ISO27001 compliance), the Processor may share a copy of the auditor's certificate, in lieu of providing other information or allowing for other audits by the controller or another auditor under this clause 4.14.

5 – Authorised disclosures

5.1) Notwithstanding any other provision of this Agreement, the Customer agrees that ETICLOUD may be required to disclose certain Personal Data (ETICLOUD will notify the Customer in any such event):

a) to Government agencies or law enforcement authorities in accordance with Applicable Law;

b) to third party providers or licensors who are required to disclose certain Personal Data to Government agencies or law enforcement authorities in accordance with Applicable Law;

c) to third party providers for the proper operation of the Services, including to third party providers of products and/or services used in the provision of the Services in connection with the provision of trouble shooting or other support services in connection therewith;

d) to third party administrators or registrars such as RIPE who require such Personal Data for the proper operation of the Services and for the provision of databases such as the WHOIS database; and/or

e) to third party licensors whose software is licensed to the Customer in connection with the provision of the Services and who require such Personal Data for licence audit purposes,

in each case where relevant to the Services provided by ETICLOUD to the Customer.

5.2) This Agreement shall be without prejudice to any obligations of the Customer under any Services Agreement or Applicable Law to provide information to ETICLOUD concerning its use of the Services.

6 – Notices

6.1) Any Notices to ETICLOUD under this Agreement should be sent by email to dpo@everythingthatis.cloud or in writing via letter to ETICLOUD Data Protection Officer, Enterprise House, Unit 1 Broadfield Court, Sheffield, S8 0XF. All notices under clauses 4.11 (Data Security Incidents) and 4.12 (Subject Access Requests) should be notified via email to dpo@everythingthatis.cloud marked as high importance.

6.2) Any notice, letter or other communication contemplated by this Agreement will be communicated in writing via letter to the addresses set out in the relevant Schedule or by email to email addresses agreed between the Parties.

7 – Miscellaneous

7.1) This Agreement and the Services Agreement shall constitute the entire agreement between the Parties relating to the subject matter of this Agreement and supersede all prior agreements, understandings, negotiations and discussions of the Parties.

7.2) The provisions of this Agreement are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this Agreement will remain in full force and effect.

7.3) The provisions of this Agreement will endure to the benefit of and will be binding upon the Parties and their respective successors and assigns.

7.4) This Agreement may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

7.5) This Agreement will be governed by and construed in accordance with the laws of England, unless a different choice of law applies under the Services Agreement, in which case the law that governs the Services Agreement shall also govern this Agreement.

7.6) The Parties agree that no person who is not a Party to this Agreement shall have the right to enforce any provision of it in accordance with the Contracts (Rights of Third Parties) Act

1999 (“**CRTPA**“). Nothing in this clause shall affect the right of any person which exists apart from the CRTPA.

etiCloud

DEFINITIONS AND INTERPRETATION

1 – Definitions

1.1) In this Agreement:

"**Adequate Territory**"	means a territory outside of the UK that has been designated by the Secretary of State under Article 45 of the UK GDPR and section 17A of the Data Protection Act 2018 as ensuring an adequate level of protection pursuant to Data Protection Law.
"this Agreement"	means this Data Processing Agreement comprising the Data Processing Terms and the Definitions and Interpretation section.
"Applicable Law"	means applicable law, statute, bye-law, regulation, order, regulatory policy, guidance or industry code, rule of court or directives or requirements of any regulatory body, delegated or subordinate legislation or notice of any regulatory body.
"**Communications Data**"	means any data processed for the purpose of the conveyance of (or billing of) any electronic communication or communication on an electronic communications network, including SMS, MMS, email and internet connection records, and any Location Data. Communications Data may include records of connections to particular telephone numbers, devices and users and the dates, times and durations of such connections.
"**Content Data**"	means the content (comprising any speech, music, sounds, visual images or data of any description) of any electronic communication by a User, including the content of electronic messages, such as SMS, MMS and email, and web pages requested to the extent that it is not Communications Data.
"**Controller**"	means an entity that alone or jointly with others determines the purposes and means of Processing of Personal Data.
"**CRM Data**"	means any Personal Data of staff or representatives of a Party which is processed by the other Party for the purposes of managing the Services, administering a Services Agreement or marketing products or services to that Party.

"**Customer**"	means the entity contracting with ETICLOUD as identified in the Services Agreement/Order Form.
"**Data Protection Law**"	means all Applicable Laws relating to data protection, the processing of personal data and privacy including: (a) the Data Protection Act 2018; (b) the UK GDPR (as defined in section 3 of the Data Protection Act 2018); (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended); and (d) any other law relating to data protection, the processing or personal data and privacy that is applicable from time to time in the UK.
"**Data Security Incident**"	means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
"**Effective Date**"	means the date of contract signing.
"**ETICLOUD**"	ETICLOUD Ltd (Co No 09777907) and any other member of the ETICLOUD group of companies as is named as the supplier of the Services in an Order Form/ the Services Agreement
"**ETICLOUD Data Processing Schedule**"	means ETICLOUD's record (available at www.everythingthatis.cloud/DPA-processingresponsibilities.pdf, as updated by ETICLOUD from time to time) describing the categories of Personal Data that it

	processes in connection with each of the services that it offers to its customers and ETICLOUD's responsibility as a Controller or Processor with respect to the processing.
"**Location Data**"	means any data processed in an electronic communications network indicating the geographic position of the terminal equipment of a User, geographic location derived from a geographic identifiers associated with the access network or any other identifiers with known or presumed coordinates for the network elements to which a User is connected.
"**Standard Data Protection Clauses**"	means standard data protection clauses under (as applicable) Article 46(2)(c) and Article 46(2)(d) of the UK GDPR as may be amended or superseded from time to time.
"**Personal Data**"	means any information relating to an identified or Identifiable natural person (including the categories of data defined in this Agreement or described in the ETICLOUD Data Processing Schedule). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to his/her physical, physiological, genetic, mental, economic, cultural or social identity.
"**Security Policy**"	means ETICLOUD's security policy which details the security measures taken by ETICLOUD in the provision of the Services and its current practices regarding the maintenance of the security of data, the current version of which may be made available on ETICLOUD's website or upon request from ETICLOUD.
"**Services**"	means the services provided by ETICLOUD to the

	Customer as more particularly described in the Services Agreement/Order Form.
"**Services Agreement**"	the Customer's contract with ETICLOUD for the provision by ETICLOUD of the Services.
"**User**"	means any end user or administrator of a Service.
"**User Data**"	means Personal Data regarding Users which is not Communications Data, Content Data or CRM Data. Such Personal Data include user IDs, passwords, authenticators, addresses (including MAC addresses, IP addresses and email addresses) and telephone numbers.

2 – Interpretation

In this Agreement:

2.1) references to the following terms shall be given their meanings under Data Protection Law: "controller", "joint controller", "processor", "data subject", "process" or "processing", "subject access request", and any other terms that are defined under Data Protection Law and used in this Agreement;

2.2) words in the singular shall include the plural and words in the plural shall include the singular unless the context requires otherwise;

2.3) headings are for convenience only and shall not affect the interpretation of this Agreement;

2.4) references to a Party include references to its successors in title and permitted assigns; and

2.5) references to "includes" or "including" shall be read as being immediately followed by the words "without limitation".

3 – Services Agreement

Except to the extent that they are inconsistent with the definitions and interpretations in the Definitions and Interpretation section of this Agreement, the definitions and interpretations in the Services Agreement shall also apply in this Agreement.


etiCloud