DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

Data Processing Addendum

This Data Processing Addendum (***"Addendum"***), applies to, and forms part of, agreements between Bettermode Inc. (***"Bettermode"***), and entities who subscribe for Bettermode's services and who are subject to Applicable Law (***"Customer"***) (collectively referred to as the ***"Parties"***), and sets forth the terms and conditions relating to the privacy, confidentiality and security of Personal Data (as defined below) associated with services to be rendered by Bettermode to Customer pursuant to the subscription agreement entered into between the Parties (the ***"Master Agreement"***). "). In the event of conflict between the terms of this Addendum and the Master Agreement, this Addendum will control and take precedence.

I. Definitions

(A) ***"Applicable Law"*** means all applicable laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the Personal Information Protection and Electronic Documents Act ("PIPEDA");the UK Data Protection Act 2018 the GDPR as it forms part of United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (the "UK GDPR"); the Swiss Federal Act on Data Protection;; the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR") as applied, supplemented, modified and/or replaced from time to time by the laws of the United Kingdom, Switzerland and/or the relevant member state of the European Union and European Economic Area (as the case may be);,; EU Directive 2002/58/EC on Privacy and Electronic Communications ("e-Privacy Directive"); the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, as amended from time to time ("the CCPA"); and any other directly applicable laws or regulation relating to privacy and data rights of natural persons having effect or enacted in the United States, Switzerland, United Kingdom, the European Economic Area, and/or the European Union or a relevant state or member state thereof (as the case may be), or anywhere else in the world, in each of the foregoing instances, as applicable to the Processing of Personal Data by Processor.

(B) ***"Data Controller"*** means a person who alone or jointly with others determines the purposes and means of the Processing of Personal Data.

(C) ***"Data Processor"*** means a person who Processes Personal Data on behalf of the Data Controller.

(D) ***"Data Security Measures"*** means technical and organisational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorised access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.

(E) ***"Data Subject"*** means an identified or identifiable natural person to which the Personal Data pertain.

(F) ***"Instructions"*** means this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.

(G) ***"Personal Data"*** and ***"Personal Information"*** means any information relating to: (i) an identified or identifiable natural person; or (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Privacy Laws), where for each (i) or (ii), such data, or any part of such data, is Processed in the performance of Services. in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental,

economic, cultural or social identity of that natural person.

(H) ***"Personal Data Breach" means*** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

(I) ***"Process", "Processed",*** or ***"Processing"*** means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(J) ***"Services"*** means the services offered by Bettermode and subscribed for by Customer under the Master Agreement.

(K) ***"Sub-Processor"*** means the entity engaged by the Data Processor or any further Sub- Processor to Process Personal Data on behalf and under the authority of the Data Controller.

(L) "Standard Contractual Clauses" means (i) where the GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation EU 2016/679 of the European Parliament and of the Council ("EU SCCs"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" issued by the Information Commissioner's Office under Section 119A(1) of the UK Data Protection Act 2018 (the "UK Addendum").

II. Roles and Responsibilities of the Parties

(A) This Addendum applies only to the extent that Provider Processes Customer Personal Data on behalf of Customer in providing the Services and where such Customer Personal Data is subject to the Applicable Laws.

(B) The Parties acknowledge and agree that Customer is acting as a Data Controller,and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data Processed under this Addendum, and Bettermode is acting as a Data Processor on behalf and under the Instructions of Customer.

(C) Any Personal Data will at all times be and remain the sole property of Customer and Bettermode will not have or obtain any rights therein.

III. Obligations of Bettermode

Bettermode agrees and warrants to:

(A) Process Personal Data disclosed to it by Customer only on behalf of and in accordance with the Instructions of the Data Controller and Annex 1 of this Addendum, unless Bettermode is otherwise required by Applicable Law. Bettermode shall inform Customer if, in Bettermode's opinion, an Instruction provided infringes Applicable Law.

(B) Ensure that any person authorised by Bettermode to Process Personal Data in the context of the Services is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Data Controller.

(C) Bettermode stores and Processes all data, including Personal Data, in the US unless agreed otherwise.

(D) Inform Customer promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and not respond to such requests, unless instructed by the Customer in writing to do so. Taking into account the nature of the Processing of Personal Data, Bettermode shall assist Customer, by appropriate technical and organisational measures and at Customer's cost, insofar as possible, in fulfilling Customer's obligations to respond to a Data Subject's request to exercise their rights with respect to their Personal Data.

(E) Notify Customer promptly and without undue in writing of any subpoena or other judicial or administrative order by a government authority or proceeding seeking access to or disclosure of Personal Data. Customer shall have the right to defend such action in lieu of and on behalf of Bettermode. Customer may, if it so chooses, seek a protective order. Bettermode shall reasonably cooperate with Customer in such defense.

(F) Provide reasonable assistance to Customer, at Customer's cost, in complying with Customer's obligations under Applicable Law.

(G) Maintain internal record(s) of Processing activities, copies of which shall be provided to Customer by Bettermode or to supervisory authorities upon request.

(H) Remain in compliance with GDPR, CCPA, PIPEDA and all other Applicable Laws with respect to any and all of Customer's users while they are using the Bettermode Services.

IV. Data storage and transfers

(A) Bettermode stores and Processes all data, including Personal Data, in the US and/or Canada. Bettermode has and shall continue to enter into any written agreements as are reasonably necessary (in its reasonable determination) to comply with Applicable Law concerning any cross-border transfer of Personal Data, whether to or from Bettermode.

(B) Where required in order to comply with Applicable Laws, including (a) the GDPR, the EU SCCs attached hereto as Exhibit A and the additional terms set forth in this Section shall apply only to Personal Data that is transferred from the EEA to outside the EEA, either directly or via onward transfer, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data, and (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data, including but not limited to Binding Corporate Rules for Processors; and (b) the UK GDPR, the UK Addendum and the additional terms set forth in this Section shall apply only to Personal Data that is transferred from the UK to outside the UK, either directly or via onward transfer, to any country or recipient which is not subject based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

(C) The Standard Contractual Clauses and the additional terms specified in this Section apply to the legal entity that has executed the Standard Contractual Clauses as a data exporter and those of its Affiliates that are subject to the Applicable Laws if and to the extent Bettermode Processes Personal Data for which such legal entity and its Affiliate(s) qualify as the Controller. For purposes of the Standard Contractual Clauses, the aforementioned entities shall be deemed "data exporters";

(D) Pursuant to Clause 5(h) of the EU SCCs, Customer agrees that Bettermode may engage Sub-processors in connection with the provision of the Subscription Services in accordance with Section V below;

(E) Customer agrees that the copies of the Sub-processor agreements to be provided by Bettermode to Customer pursuant to Clause 5(j) of the EU SCCs (where applicable) may have all commercial information, or clauses unrelated to the EU SCCs or their equivalent, removed by Bettermode, and such copies will be provided by Bettermode only upon written request by Customer and subject to any obligations of confidentiality to which Bettermode may be bound, and further provided, if Bettermode is contractually restricted from disclosing any such agreements to Customer, Bettermode will use reasonable efforts to require such Sub-processor to permit it to disclose the agreement to Customer; Customer agrees that the certification of deletion of Personal Data that is described in Clause 12(1) of the EU SCCs shall be provided by Bettermode to Customer only if requested by the Customer in writing.

(F) In relation to Personal Data that is protected by the UK GDPR, the parties agree as follows (a) the EU SCCs, completed as set out in the Appendix — Annex 1 and Annex 2 shall apply, and the EU SCCs will be deemed amended as specified by Part 2 of the UK Addendum, which will be deemed entered into and incorporated into this Addendum by this reference; (b) Tables 1 to 3 in Part 1 of the UK Addendum shall be deemed completed with the relevant information from the EU SCCs, completed as set out in Annex I of this Addendum (as applicable); and (c) the option "Exporter" shall be deemed checked in Table 4 in Part 1 of the UK Addendum

V. Sub-Processing

(A) Bettermode shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless Bettermode has entered into a written agreement with each such third party that imposes obligations on the third party that are substantively similar as those imposed on Bettermode under this Addendum. Bettermode shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data. A list of Bettermode's current Sub-Processors are set out at [https://bettermode.com/subprocessors]. Bettermode shall provide Customer with thirty (30) days' prior notice before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services, giving Customer reasonable opportunity to object to the appointment of such Sub-processor(s).

(B) Where Customer permits the integration of the Service with third party services, such integration may allow for the transfer of data to such third party (subject to Customer's consent through the configuration of the integration by Customer). Such third parties shall not be considered Sub-Processors for the purpose of this section and it is Customer sole obligation to ensure that it has the appropriate agreements in place with such third party in respect of the processing of such data.

VI. Compliance with Applicable Laws

(A) Each party covenants and undertakes to the other that it shall comply with all Applicable Laws in the use of the Services.

(B) Without limiting the above, (i) Customer is responsible for ensuring that it has a lawful basis for the processing of Personal Information in the manner contemplated by this Agreement, and has adequate record of such basis (whether directly or through another third party provider); and (ii) Bettermode is not responsible for determining the requirements of laws applicable to Customer's business or that Bettermode's provision of the Services meet the requirements of such laws. As between the parties, Customer is responsible for the lawfulness of the Processing of the Customer Personal Data. Customer will not use the Services in conjunction with Personal Data to the extent that doing so would violate applicable Data Protection Laws.

(C) If a Data Subject brings a claim directly against Bettermode for a violation of their Data Subject rights in breach of Applicable Laws and such claim does not arise from a breach by Bettermode of the terms of this Agreement, Customer will indemnify Bettermode for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that Bettermode has notified Customer about the claim and given Customer the opportunity to cooperate with Bettermode in the defense and settlement of the claim. Subject to the terms of the Agreement, Customer may claim from Bettermode amounts paid to a Data Subject for a violation of their rights caused by Bettermode's breach of its obligations under Applicable Law, including the GDPR and UK GDPR.

VII. Data Security

(A) Bettermode shall develop, maintain and implement a comprehensive written information security program that complies with Applicable Law and good industry practice. Bettermode's information security program shall include appropriate administrative, technical, physical, organisational and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:

a) The encryption of the Personal Data;

b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

c) The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and

d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures adopted pursuant to this provision for ensuring the security of the Processing.

(B) Bettermode shall supervise Bettermode personnel to the extent required to maintain appropriate privacy, confidentiality and security of Personal Data. Bettermode shall provide training, as appropriate, to all Bettermode personnel who have access to Personal Data.

(C) Promptly (and in any event within 90 days) following the expiration or earlier termination of the Master Agreement, Bettermode shall return to Customer or its designee, if so requested during such period, or if not so requested securely destroy or render unreadable or undecipherable, each and every original and copy in every media of all Personal Data in Bettermode's, its affiliates' or their respective subcontractors' possession, custody or control. In the event applicable law does not permit Bettermode to comply with the delivery or destruction of the Personal Data, Bettermode warrants that it shall ensure the security and confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum.

VIII. Data Breach Notification

(A) Bettermode shall promptly and without undue delay inform Customer in writing of any Personal Data Breach of which Bettermode becomes aware. The notification to Customer shall include all available information regarding such Personal Data Breach, including information on:

a) The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records;

b) The likely consequences of the Personal Data Breach; and

c) The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Bettermode shall cooperate fully with Customer in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach, to notify affected Data Subjects if required by Applicable Law, and to take all other actions required under Applicable Law as a result of the Personal Data Breach. Bettermode shall provide such assistance as required to enable Customer to satisfy Customer's obligation to notify the relevant supervisory authority and Data Subjects of a personal data breach under Articles 33 and 34 of the GDPR or other Applicable Laws, if applicable.

IX. Audit

Bettermode shall on written request (but not more than once per year, other than in the event of a breach) make available to Customer such information as may be reasonably necessary to demonstrate compliance with the obligations set forth in this Addendum and, where required by Applicable Law and at the Customer's expense, allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer. Upon prior written request by Customer (provided that it shall be not more than once per year other than in the event of a breach), Bettermode agrees to cooperate and, within reasonable time, provide Customer with: (a) audit reports (if any) and all information necessary to demonstrate Bettermode's compliance with the obligations laid down in this Addendum; and (b) confirmation that no audit, if conducted, has revealed any material vulnerability in Bettermode's systems, or to the extent that any such vulnerability was detected, that Bettermode has fully remedied such vulnerability.

X. Governing Law

This Addendum shall be governed by the laws of the jurisdiction specified in the Agreement.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

ANNEX 1: SCOPE OF THE DATA PROCESSING SCOPE OF THE

DATA PROCESSING

This Annex forms part of the Data Processing Addendum between Customer and

Bettermode.

The Processing of Personal Data concerns the following categories of Data

Subjects: End users and Customer's administrative users

The Processing concerns the following categories of Personal Data:

(i) Name: To help data subjects identify themselves in the community and let others call them by their names or nicknames
(ii) External user ID (Optional): To uniquely identify the data subject when the data subject is authenticated
(iii) Email address: To send email notifications to data subjects
(iv) Biography: For data subjects to introduce themselves to the community
(v) Profile Pictures: For data subjects to introduce themselves to the community by uploading their picture or Avatar
(vi) IP addresses: To log data subjects activities for future reference and to secure the community in case of spam attacks from a certain IP
(vii) Cookie data: sessionId for authentication purpose and CSRF-Token for security purpose
(viii) Behavioral Events: To enhance user experience and show the most relevant and recommended content to the data subjects

(ix) Posts, replies, uploaded files and videos of data subjects: To provide the community services to data subjects.

(X) such additional ad hoc categories as may be prompted by new fields added by Customer.
The Processing concerns the following categories of Sensitive Data:

None.

The Processing concerns the following categories of data Processing activities (i.e., purposes of Processing):
Provision of services to Customer and Customer's end users

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

ANNEX 2

EU SCCs (PROCESSORS)

According to COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

SECTION I

Clause 1
Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2
Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3
Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional
Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of noncompliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
Use of sub-processors

(a) The data importer shall not subcontract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 14 (fourteen) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15
Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the re-questing authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16
Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18
Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Customer, a user of the Services.

Name: _____
Address: _____

Signature and date: _____

_____

Role (controller)

Data importer(s): Bettermode Inc., provider of the Subscription Services.

Name: Bettermode Inc.
Address: 1607 - 22 Wellesley St. East, Toronto, ON, M4Y 1G3 Canada
Data protection officer: Siavash Mahmoudian dpo@bettermode.com

Signature and date: 12/8/2022

DocuSigned by:
Siavash Mahmoudian
16E9562E58C24B8...

Role (processor)

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

End users and Customer's administrative users

Categories of personal data transferred

- Name: To help data subjects identify themselves in the community and let others call them by their names or nicknames
- (ii) External user ID (Optional): To uniquely identify the data subject when the data subject is authenticated
- (iii) Email address: To send email notifications to data subjects
- (iv) Biography: For data subjects to introduce themselves to the community
- (v) Profile Pictures: For data subjects to introduce themselves to the community by uploading their picture or Avatar
- (vi) IP addresses: To log data subjects activities for future reference and to secure the community in case of spam attacks from a certain IP
- (vii) Cookie data: sessionId for authentication purpose and CSRF-Token for security purpose
- (viii) Behavioral Events: To enhance user experience and show the most relevant and recommended content to the data subjects
- (ix) Posts, replies, uploaded files and videos of data subjects: To provide the community services to data subjects.

The frequency of the transfer*:*

Continuous

Purpose(s) of the data transfer and further processing

Provision of services to Customer and Customer's end users

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Continuously during the terms of service

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

Requests for access to Bettermode Platform systems and applications are made formally using the following process:

1. A Bettermode workforce member initiates the access request by creating an Issue in the Bettermode ticketing system.
    1. User identities must be verified prior to granting access to new accounts.
    2. Identity verification must be done in person where possible; for remote employees, identities must be verified over the phone.
    3. For new accounts, the method used to verify the user's identity must be recorded on the Issue.
2. The Security Officer will grant or reject access to systems as dictated by the employee's job title. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request.
3. If the request is rejected, it goes back for further review and documentation.
4. If the review is approved, the request is marked as “Done”, and any pertinent notes are added.

Access Reviews

All access to Bettermode systems and services is reviewed and updated on a **quarterly** basis to ensure proper authorizations are in place commensurate with job functions. The process for conducting reviews is outlined below:

1. The Security Officer initiates the review of user access by creating an Issue in the Bettermode Ticketing System
2. The Security Officer is assigned to review levels of access for each Bettermode workforce member.
3. If user access is found during review that is not in line with the least privilege principle, the Security Officer may modify user access and notify the user of access changes.
4. Once the review is complete, the Security Officer then marks the ticket as “Done”, adding any pertinent notes required.

Workforce Clearance

- The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification.
- All access requests are treated on a **"least-access principle."**
- Bettermode maintains a minimum necessary approach to access to Customer data.

Unique User Identification

- Access to the Bettermode Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
- Passwords requirements mandate strong password controls.
- Passwords are not displayed at any time and are not transmitted or stored in plain text.
- Default accounts on all production systems, including root, are disabled.
- Shared accounts are not allowed within Bettermode systems or networks.
- Automated log-on configurations other than the company’s approved Password Management provider that store user passwords or bypass password entry are not permitted for use with Bettermode workstations or production systems.

Automatic Logoff

- Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).

Employee Workstation Use

All workstations owned by Bettermode, are laptop products running Windows, Mac OSX or Linux.

- Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.

- Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through the organization's system.
- Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
- Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
- Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
- Workstation hard drives must be encrypted
- All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.

All other workstations owned by individuals, are products running Windows, Mac OSX or Linux.

- Any use of organization's information systems/applications for personal gain is prohibited.
- Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
- Workstation hard drives must be encrypted
- All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.

Employee Termination/Offboarding Procedures

1. The Human Resources Department (or other designated department), users, and their supervisors are required to notify the Security Officer upon completion and/or termination of access needs and facilitate completion of the "Termination Checklist".
2. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):
    1. The user has been using their access rights inappropriately;
    2. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
3. The Security Officer will terminate users' access rights within **24 hours** of termination/separation, and will coordinate with the appropriate Bettermode employees to terminate access to any non-production systems managed by those employees.
4. The Security Officer audits and may terminate access of users that have not logged into the organization's information systems/applications for an extended period of time.

DocuSign Envelope ID: 59AA4EA1-9339-4BB3-8B36-0D7B76DAD3D2

ANNEX III – LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors listed at https://bettermode.com/subprocessors