DATA PROCESSING ADDENDUM

Data Privacy			
Subject Matter, Nature, and Purpose of Processing	The provision of Subscription Services to Customer	**Duration**	Term of the Agreement
Type of Personal Data to be Processed	Communication data (e.g., telephone number, mobile phone number, call detail records, email); business and personal contact details (e.g., name, postal address); and other Personal Data submitted to the Subscription Service.	**Categories of Data Subjects**	Clients and other business contacts; Employees and contractors; Subcontractors and agents; and Consultants and partners.

This Data Processing Addendum ("**DPA**") is incorporated into, and forms part of, the Master Ordering Agreement between MobiChord, Inc. d/b/a brightfin, a Delaware corporation ("**brightfin**") and _____ ("**Customer**") dated as of _____ (the "**Agreement**") and applies where brightfin acts as a Processor in the provision of Subscription Services under the Agreement. Capitalized terms that are not defined in this DPA have the meanings ascribed to them in Data Protection Laws or the Agreement. In the event of any conflict between the Agreement and this DPA, the provisions of this DPA will prevail.

1. **Definitions.**

   1.1. **"Data Protection Laws"** means any data protection legislation or regulation applicable to the Processing of Personal Data by brightfin under the Agreement, including, as applicable: (i) the General Data Protection Regulation (EU) 2016/679 ("**EU GDPR**"); (ii) the General Data Protection Regulation as it forms part of UK domestic law by virtue of the UK Data Protection Act 2018 and Section 3 of the European Union (Withdrawal) Act 2018 and subsequent amendments ("**UK GDPR**"); (iii) the California Consumer Privacy Act of 2018, as amended or modified, including as amended by the California Privacy Rights Act of 2020 ("**CCPA**"); (iv) Colorado Privacy Act (Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313) ("**ColoPA**"); (v) Connecticut Personal Data Privacy and Online Monitoring Act (Public Act No. 22-15) ("**CPOMA**"); (vi) Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404) ("**UCPA**"); and (vii) Virginia Consumer Data Protection Act (Virginia Code Ann. §§ 59.1-575 to 59.1-585) ("**VCDPA**"). Unless otherwise stated, "**GDPR**" means both the EU GDPR and UK GDPR. Notwithstanding the foregoing, "Data Protection Laws" shall not include any laws or regulations that require the localisation of Personal Data.

   1.2. "**Personal Data**" means any information relating to an identifiable or identified Data Subject that **(i)** brightfin processes as a Processor while providing Customer with the Subscription Services under the Agreement, and **(ii)** would be considered personal information or personal data as such terms/concepts are defined by applicable Data Protection Laws; provided, however, that Personal Data excludes any such information that has been aggregated or anonymized in a manner that is not **(A)** identifiable as having originated from the Data Subject, or **(B)** capable of allowing a recipient to infer the Data Subject's information.

   1.3. "**Controller**", "**Data Subject**", "**Processor**" and "**Processing**" have the meanings ascribed to them in the GDPR and their cognate terms will be construed accordingly.

   1.4. "**Subprocessor**" means an entity appointed by brightfin to Process Personal Data on behalf of Customer in connection with the Agreement and excludes third party contributions, features, functionality, consulting or other third-party services elected by Customer.

2. **Roles and Processing**. brightfin shall act as Processor and Process the Personal Data only to provide the Subscription Services, on Customer's documented instructions, or as consistent with the Agreement. Customer shall act as Controller and shall comply with all applicable laws, including Data Protection Laws, in providing Personal Data to brightfin and further represents and warrants that all Personal Data will be collected and used by or on behalf of Customer in compliance with such laws, including with respect to any applicable obligations to provide notice to and/or obtain consent from individuals.

3. **Subprocessing.** brightfin may use Subprocessors to process the Personal Data in compliance with Data Protection Laws. brightfin's current Subprocessors are set forth at https://www.brightfin.com/sub-processors/, or its successor page.

   3.1. **Additions; Replacement.** This DPA is Customer's general written authorization for brightfin to engage Subprocessors; provided, however, that brightfin will inform Customer through Customer's primary contact or by posting on Customer's control panel any intended changes concerning the addition or replacement of Subprocessors. If, within 14 days of

receiving such notice, Customer does not provide written notice to brightfin of any reasonable objections that detail why the proposed Subprocessor would not adequately support Customer's obligations under the Data Protection Laws, Customer will be deemed to have consented to the proposed engagement. If the parties are not able to resolve a reasonable objection and brightfin continues to appoint such Subprocessor, then Customer will be entitled to terminate any agreements with respect to the processing of Personal Data under the Data Protection Laws by the new Subprocessor without any liability as a result of such termination (such termination, a "**Subprocessor Objection Termination**"). For the avoidance of doubt, brightfin shall have no liability for a Subprocessor Objection Termination and such Subprocessor Objection Termination shall not constitute a termination for breach.

3.2. **Liability.** brightfin shall conduct security, privacy, and transfer assessments of all Subprocessors prior to onboarding and will enter into written agreements with any Subprocessor requiring the Subprocessor to provide a substantially similar level of data protection and information security as provided by this DPA and required by Data Protection Laws. brightfin will remain liable for any Subprocessor's compliance with its obligations and for any acts or omissions of a Subprocessor that cause a Subprocessor to fail to fulfill such obligations or that cause brightfin to breach any of its material obligations under this DPA.

4. **Confidentiality.** brightfin will treat all Personal Data that it Processes as confidential and will inform its employees, agents and/or approved Subprocessors engaged in Processing Customer Personal Data of the confidential nature of the Personal Data. brightfin will make commercially reasonable efforts to ensure that these persons or entities have signed an appropriate confidentiality or data protection agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

5. **Security.** brightfin will implement the measures set forth in **Exhibit A** and not less than appropriate technical and organizational measures to protect the security of the Processing of Personal Data, taking 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.

6. **Assistance/Inspections.** brightfin will make relevant information necessary to demonstrate compliance with Article 28 of the GDPR reasonably available. At Customer's written request, brightfin will, taking into account the nature of processing and the information available to the processor, reasonably assist the Customer in ensuring compliance with obligations pursuant to Articles 32 to 36 of the GDPR.

   6.1. For the avoidance of doubt**,** Customer agrees and understands that brightfin's most recent third-party audit attestations, certifications, and reports, will suffice for purposes of any required documentation under this provision.

   6.2. To the extent the documentation identified in Section 6.1 does not provide sufficient information under Data Protection Laws, then brightfin will, at Customer's expense and subject to reasonable notice, scope, frequency, relevancy, and confidentiality requirements, allow for and contribute to audits, including inspections, conducted by Customer or an appropriately-qualified auditor, provided that the information sought is not reasonably available through less intrusive means. Customer will reimburse brightfin for any time expended on such audits or inspections.

7. **Data Subject Requests.** To the extent possible and taking into account the nature of the processing, brightfin will make commercially reasonable efforts to assist Customer by providing functionality or taking appropriate measures to help fulfill Customer's obligation to respond to Data Subject requests under applicable Data Protection Laws.

8. **Notifications.** If brightfin is otherwise required to comply with a legal obligation, brightfin will make commercially reasonable efforts to inform Customer of that legal obligation, unless brightfin is prohibited from doing so. brightfin will inform Customer if, to its knowledge, an instruction from Customer would infringe Data Protection Laws.

9. **Incident Management.** If brightfin becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed by brightfin under this DPA while providing the Subscription Services (a "**Security Incident**"), it will, without undue delay, notify Customer and provide Customer a description of the Security Incident as well as periodic updates to information about the Security Incident, brightfin will investigate the Security Incident and take reasonable steps to prevent or mitigate the effects of a Security Incident caused by a material breach of brightfin's obligations under this DPA.

10. **Sensitive Data.** Except as specifically provided otherwise, the Subscription Services are not intended to store any type of Sensitive Personal Data, including any data that may be considered "special categories of personal data" under Data Protection Laws, or that otherwise would reasonably be considered sensitive in nature (collectively, "**Sensitive Data**"). For example, the Subscription Services are not intended to store or use sensitive health data, including but not limited to protected health information ("**PHI**"), as defined by the Health Insurance Portability and Accountability Act of 1996 and its

enabling regulations and related laws ("**HIPAA**"). Customer will not provide brightfin with any Sensitive Data through use of the Subscription Services.

11. **Data Transfer.** brightfin may transfer, process and store Personal Data in regions in which brightfin or its Subprocessors operate, subject to compliance with Data Protection Laws.

11.1. If and to the extent that any processing of Personal Data subject to the EU GDPR by brightfin takes place in any country outside the EEA whose laws do not provide an adequate level of data protection and an independently valid data transfer mechanism does not exist, or either party relies on a transfer mechanism that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, then:

a) the parties will, to the extent necessary, cooperate in good faith to terminate the transfer or pursue a suitable alternate mechanism that can lawfully support the transfer; and

b) the Standard Contractual Clauses approved by the European Commission on 4 June 2021 under Commission Implementing Decision (EU) 2021/914, Controller-to-Processor Clauses (Module Two) ("**EU SCCs**") will apply:

i. for the purposes of Annex I to the EU SCCs, brightfin will comply with the obligations of "data importer" and the Customer will comply with the obligations of "data exporter;"

ii. the activities of Customer as data exporter, of brightfin as data importer, and the details of the data subjects, types of data, special categories of data (if appropriate) and processing operations are as set out throughout this DPA and in the table on page 1 of this DPA;

iii. Clause 3 of this DPA (Subprocessing) shall apply for purposes of Annex III to the EU SCCs and for general written authorization of sub-processors under Clause 9(a) of the EU SCCs (Use of sub-processors);

iv. the laws of the Republic of Ireland will govern the EU SCCs (Clause 17) and that the choice of forum and jurisdiction shall be the courts of the Republic of Ireland (Clause 18(b));

v. for the purposes of Annex I.C. (Competent Supervisory Authority), the competent supervisory authority is Data Protection Commission, Ireland; and

vi. Exhibit A of this DPA shall apply for the purposes of Annex II to the EU SCCs (Technical and Organisational Measures).

11.2. If and to the extent that any processing of Personal Data subject to the UK GDPR by brightfin takes place in any country outside the UK whose laws do not provide an adequate level of data protection and an independently valid data transfer mechanism does not exist, or either party relies on a statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, then:

a) the parties will, to the extent necessary, cooperate in good faith to terminate the transfer or pursue a suitable alternate mechanism that can lawfully support the transfer; and

b) the terms of the International Data Transfer Addendum to the EU SCCs in force 21 March 2022 issued by the UK Information Commissioner's Office pursuant to S119A(1) of the UK Data Protection Act 2018 ("**UK IDTA**") will apply:

i. for purposes of Part I of the UK IDTA, the terms of this DPA, including the relevant roles of the parties as set forth in Section 11.2(b) and the technical and organizational measures set out in Exhibit A, shall apply;

ii. both Customer and brightfin shall be allowed to end subscription to the UK IDTA as set out in Section 19 of the UK IDTA; and

iii. for purposes of Part 2 of the UK IDTA, the EU SCCs shall apply.

11.3. If and to the extent that any processing of Personal Data subject to the jurisdiction of the Swiss Federal Data Protection and Information Commission ("**FDPIC**") takes place in any country outside Switzerland whose laws do not provide an adequate level of data protection and an independently valid data transfer mechanism not exist, or either party relies on a statutory mechanism to normalize international data transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, then

a) the parties will, to the extent necessary, cooperate in good faith to terminate the transfer or pursue a suitable alternate mechanism that can lawfully support the transfer; and

b) the EU SCCs and cognate roles, activities, and authorizations set forth in Section 11.2(b) will apply, except that:

i. all references to the GDPR shall be read to include reference to the Swiss Data Protection Act; and

ii. the competent supervisory authority shall be the FDPIC.

11.4. brightfin will notify Customer if it can no longer meet its obligation to provide the level of protection required by Data Protection Laws.

12. **CCPA Compliance**. If brightfin Processes Personal Data of California residents, brightfin shall comply with the CCPA. Specifically, brightfin agrees that:

12.1. brightfin acts solely as a Service Provider in relation to Personal Data ("**Service Provider**" shall have the meaning ascribed to in the CCPA) and, in accordance with the provisions of this DPA, Customer alone determines the purposes and means of the Processing of Personal Data.

12.2. brightfin will not sell Personal Data of California residents, and the parties acknowledge and agree that Customer does not sell Personal Data to brightfin in connection with the Subscription Services. Further, as set forth elsewhere in this DPA, brightfin will not retain, use, share, or disclose Customer Personal Data (1) for any purpose other than performing or supporting the Subscription Services, or (2) outside of the direct business relationship between the parties except as authorized through the Agreement. When utilizing Subprocessors to perform or support the Subscription Services, brightfin will comply with the provisions of Section 3 of this DPA.

12.3. For the purposes of data security under the CCPA, brightfin shall comply with the applicable requirements and restrictions set forth in the Agreement and this DPA, including Exhibit A.

13. **Termination.** Upon termination of the Subscription Services or expiration of the Term, subject to Data Protection Laws, brightfin will promptly delete or anonymize Personal Data. If Customer requests a copy of such Personal Data prior to deletion, brightfin will make a copy of such Personal Data reasonably available to Customer.

14. **Updates**. Subject to compliance with Data Protection Laws, brightfin may update this DPA periodically, including as necessary to account for changes in circumstances, Data Protection Laws, international data transfer mechanisms, and brightfin products, features, or functionality. brightfin will not materially decrease the overall level of data protection provided by this DPA without advance notice.

Customer:		**brightfin:**	
By:	_____	**By:**	_____
Name:	_____	**Name:**	_____
Title:	_____	**Title:**	_____
Date:	_____	**Date:**	_____

Exhibit A
Technical and Organizational Measures

- Pseudonymization and encryption of Personal Data
- Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- Ability to restore the availability of and access to Customer Personal Data in a timely manner following a physical or technical incident:
- Regular testing, assessment, and evaluation of the effectiveness of technical and organizational measures used to secure Processing
- User identification and authorization process and protection
- Protecting Customer Personal Data during transmission (in transit)
- Protecting Customer Personal Data during storage (at rest)
- Physical security where Customer Personal Data is processed:
- Events logging
- Systems configuration, including default configuration
- Internal IT and IT security governance and management
- Allowing data portability and ensuring erasure

End