

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this “**DPA**”) forms part of the agreement that governs Customer’s access to and use of the Libsyn Platform and Services, including any applicable Master Terms and Conditions, Order Document, Service Terms, or other agreement between Customer and Webmayhem, Inc., doing business as Liberated Syndication and Libsyn (“**Libsyn**”) (collectively, the “**Agreement**”). This DPA is effective on the effective date of the Agreement. Capitalized terms not defined in this DPA have the meanings given in the Agreement.

1. DEFINITIONS

1.1 Aggregated and Deidentified Data means information derived from Customer Personal Information that Libsyn has aggregated, deidentified, or both, in accordance with Applicable Data Protection Laws, and does not identify, and cannot reasonably be linked to, any individual, household, or device; provided that Libsyn shall not disclose such data externally in a manner that identifies Customer or an individual or household without the applicable party’s authorization.

1.2 Applicable Data Protection Law means all laws and binding regulations applicable to a party’s Processing of Personal Data under the Agreement, including, as applicable, the GDPR, UK GDPR, Swiss Federal Act on Data Protection, CCPA (and other US State consumer privacy laws, as applicable).

1.3 CCPA means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act, and its implementing regulations.

1.4 Customer Content (or Your Content) means any and all podcasts, metadata, audio files, video files, attachments, text, images, advertising creative, and other materials that Customer uploads, submits, or makes available in connection with Customer’s use of the Libsyn Platform.

1.5 Customer Personal Data means Personal Data that Libsyn Processes on behalf of Customer in its capacity as a Processor or Service Provider to provide the Processor Activities identified in Section 3 and Schedule 1. Customer Personal Data excludes Libsyn Controller Data, Aggregated and Deidentified Data, and data for which Libsyn does not act as Customer’s Processor or Service Provider under Applicable Data Protection Law.

1.6 EEA means the European Economic Area.

1.7 EU SCCs means the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914, as amended, replaced, or superseded.

1.8 GDPR means General Data Protection Regulation (EU) 2016/679.

1.9 Independent Controller means a Controller that independently determines the purposes and essential means of its Processing. References to the parties as Independent Controllers do not create a joint-controller relationship.

1.9 Libsyn Controller Data means Personal Data that Libsyn Processes as an independent Controller for the purposes described in Section 4 and Schedule 2, including applicable account, business-contact, service-usage, security, network, listener-interaction, measurement, advertising and monetization, payment, compliance, and platform data. Libsyn Controller Data does not include Customer Personal Data while Libsyn is Processing that data solely as a Processor.

1.10 Libsyn Content. means all text, graphics, user interfaces, visual interfaces, photographs, trademarks, logos, sounds, music, artwork, and computer code, including the design, structure, selection, coordination, expression, look and feel, and arrangement thereof, contained on the Libsyn Website, exclusive of Your Content.

1.11 Personal Data means information defined as “personal data,” “personal information,” or a substantially equivalent term under Applicable Data Protection Law.

1.12 Personal Data Breach means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Libsyn as a Processor. It does not include unsuccessful attempts or activities that do not compromise Customer Personal Data, such as pings, denial-of-service attempts, port scans, unsuccessful log-in attempts, or other network attacks.

1.13 Process, Processing, Controller, Processor, Data Subject, Supervisory Authority, Sell, Share, Business, Service Provider, Contractor, and Sub-processor have the meanings given under Applicable Data Protection Law. “Controller” includes a “Covered Business” where appropriate, and “Processor” includes a “Service Provider” or “Contractor” where appropriate.

1.14 Processor Activities means the Services and associated Processing that Libsyn performs on Customer’s behalf as a Processor described in Section 3 and Schedule 1.

1.15 Restricted Transfer means a cross-border transfer of Personal Data that requires an approved transfer mechanism under the GDPR, UK GDPR, or Swiss Federal Act on Data Protection.

1.16 Third-Party Platform means a third-party service, directory, application, advertising exchange, demand-side or supply-side platform, streaming service, social network, website, or other destination or integration to which Customer elects to distribute, transmit, or make available Customer Content or related data.

1.17 UK Addendum means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.

1.18 UK GDPR means the GDPR as incorporated into United Kingdom law by the European Union (Withdrawal) Act 2018, as amended.

2. PARTIES’ ROLES; ORDER OF PRECEDENCE

2.1 Parties’ Roles. For the Processing of Customer Personal Data and the activities described in Section 3 and Schedule 1, Libsyn acts as a Processor or Service Provider and Customer acts as a Controller or Covered Business. For the Processing of Libsyn Controller Data and activities described in Section 4 and Schedule 2, Libsyn acts as an Independent Controller or Covered Business.

2.3 Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (i) the applicable terms in the Standard Contractual Clauses, (ii) the terms of this DPA and (iii) the Agreement.

3. LIBSYN AS PROCESSOR OR SERVICE PROVIDER

3.1 Processing Activities. Libsyn acts as Customer's Processor or Service Provider when it Processes Customer Personal Data on Customer's behalf to: (a) host, store, cache, copy, reproduce, encode, transcode, digitize, convert, normalize, or technically modify Customer Content; (b) publish, distribute, transmit, make available, or deliver Customer Content and Customer-designated feeds; (c) operate customer-configured subscriber, premium-content, audience-contact, support, campaign, or similar features; (d) transmit Customer Content and related data to a Third-Party Platform selected or enabled by Customer; (e) provide Customer-requested reports or analytics using Customer-supplied lists or identifiers; and (f) otherwise perform a Processing activity expressly identified as Processor Processing in an Order Document or Service Terms.

3.2 Documented Instructions. Customer instructs Libsyn to Process Customer Personal Data to provide, operate, maintain, secure, and support the Processor Activities; to perform Customer's configurations and enabled features; to comply with the Agreement; and as further documented through Customer's lawful use of the Libsyn Platform, support requests, and written instructions accepted by Libsyn. Libsyn will Process Customer Personal Data only on those instructions unless Applicable Data Protection Law requires otherwise.

3.3 Unlawful Instructions. Libsyn will promptly inform Customer if, in Libsyn's sole and reasonable opinion, an instruction infringes Applicable Data Protection Law. Libsyn may suspend the affected Processing until the parties resolve the issue. Libsyn is not required to perform an instruction that is technically infeasible, would materially alter the Services, would violate law or third-party rights, or falls outside the Agreement unless the parties agree in writing to the scope, fees, and implementation.

3.4 Purpose Limitation. Libsyn will not retain, use, or disclose Customer Personal Data outside the direct business relationship with Customer or for a purpose other than the business purposes specified in the Agreement and this DPA, except as permitted or required by Applicable Data Protection Law. For clarity, Libsyn's Processing to detect security incidents, prevent fraud or illegal activity, maintain service quality and safety, debug, provide technical support, or comply with law is within Libsyn's Processing as a Controller the parties' business relationship to the extent recognized by Applicable Data Protection Law.

3.5 CCPA Restrictions. For Customer Personal Data subject to the CCPA, Libsyn certifies that it understands and will comply with the restrictions applicable to a Service Provider or Contractor. Further, Libsyn: (a) will not Sell Customer Personal Data to a third party for valuable consideration or Share Customer Personal Data to a third party for cross-context behavioral advertising; (b) retain, use, or disclose it for a commercial purpose other than the business purposes specified in the Agreement; (c) combine Customer Personal Data with Personal Data received from or on behalf of another person or collected from Libsyn's own interaction with a consumer; (d) not attempt to re-identify any pseudonymized, anonymized, aggregate or de-identified Customer Personal Data without Client's express written permission except as permitted by the CCPA; (e) provide the same level of protection for Customer Personal Data as applicable to Client; (f) notify Customer if Libsyn engages another Service Provider or Contractor to Process Customer Personal Data on behalf of Customer; (g) upon reasonable prior notice, permit Customer to monitor Libsyn's compliance with its obligations under this DPA or CCPA through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months; and (h) promptly notify Customer if Libsyn determines that it (i) can no longer meet its obligations under this DPA or CCPA, or (ii) has breached this DPA and shall cooperate to remediate such breach. Customer may take reasonable and appropriate steps to help ensure that Libsyn uses Customer Personal Data consistently with Customer's obligations and may, on reasonable notice, require Libsyn to stop and remediate unauthorized use.

3.6. Aggregated and Deidentified Data. Libsyn may create Aggregated and Deidentified Data from Customer Personal Data Processed in connection with the Services, and Libsyn may use and disclose such data for its lawful business purposes, including to operate, maintain, secure, analyze, develop, and improve its products and services; conduct research and analytics regarding the performance of the Services; and generate industry insights and benchmarking reports. Any such Aggregated and Deidentified Data shall be maintained and used in accordance with Applicable Data Protection Laws, and Libsyn will implement appropriate technical safeguards, business processes, and public commitments that reasonably prevent reidentification. Libsyn shall not use or disclose any Aggregated and Deidentified Data in a manner that identifies Customer or any individual or household and shall not attempt to re-identify Aggregated and Deidentified Data, except as permitted by applicable law or expressly authorized in writing by Customer.

3.7 Confidentiality. Libsyn will ensure that personnel authorized to Process Customer Personal Data are subject to appropriate confidentiality obligations and receive privacy and security training appropriate to their roles.

3.8 Customer Responsibilities. Customer is responsible for: (a) the lawfulness, fairness, accuracy, quality, and transparency of its Processing and instructions; (b) providing all required notices and obtaining all required consents or other legal bases for Libsyn's Processing of Customer Personal Data; (c) configuring the Services consistently with its legal obligations; (d) responding to Data Subjects except to the extent this DPA requires Libsyn's assistance; and (e) ensuring that Customer Personal Data does not include prohibited data under Section 5. Customer represents that it has all rights and permissions necessary to provide Customer Personal Data and Customer Content to Libsyn and to instruct the Processing described in this DPA.

4. LIBSYN AS INDEPENDENT CONTROLLER

4.1 Independent Purposes. Libsyn acts as an Independent Controller to the extent it determines the purposes and essential means of Processing of Libsyn Controller Data and includes one or more of the following purposes: (a) establishing and administering the commercial relationship, accounts, billing, collections, tax, and business communications; (b) authenticating users and securing the Libsyn Platform, Services, accounts, networks, and content; (c) detecting, investigating, preventing, and remediating fraud, abuse, bots, scraping, malware, unauthorized access, policy violations, Invalid Activity (as defined in the Master Terms and Conditions), and other unlawful or harmful conduct; (d) operating, monitoring, debugging, maintaining, and improving the Libsyn Platform and Services; (e) measuring content delivery, downloads, reach, attribution, and audience engagement, including applying industry-standard measurement and filtering rules; (f) creating and using Aggregated and Deidentified Data; (g) complying with law, legal process, contractual obligations, Third-Party Platform requirements, and industry standards; (h) protecting the rights, property, safety, and integrity of Libsyn, Customer, users, listeners, Third-Party Platforms, and the public; and (i) conducting advertising and monetization activities that Customer affirmatively enables or that an applicable Order Document or Service Terms expressly authorizes.

4.2 Network and Listener Data. When an end listener requests, streams, downloads, or otherwise interacts with hosted content, Libsyn may directly collect network and device data such as listener and audience data, platform telemetry, download logs, usage data, device data, IP-derived data, advertising data, analytics, performance data, attribution data, and operational data. Libsyn acts as an Independent Controller when it uses that data for platform security, fraud and bot detection, Invalid Activity detection, technical operations, legal compliance, industry-standard audience measurement, attribution, creation of Aggregated and Deidentified Data, and the other purposes in Section 4.1. Customer remains a separate independent Controller for its own collection and use of listener data and for the reports, statistics, or insights it receives from Libsyn.

4.3 Analytics and Product Improvement. The Analytics, Advertising, and Product Improvement rights in the Agreement authorize Libsyn to use Customer Content and data contained in, derived from, or generated through Customer Content and use of the Services for analytics, platform monitoring, fraud prevention, Invalid Activity detection, attribution, audience measurement, legal and platform compliance, and improvement of the Services. To the extent those activities involve Customer Personal Data and Libsyn determines their purposes and essential means, Libsyn acts as an Independent Controller. Libsyn may also use Aggregated and Deidentified Data for research, analytics, benchmarking, service development, and other lawful purposes without restriction under this DPA, subject to applicable deidentification requirements.

4.4 Advertising and Monetization. Libsyn will use Customer Content or related data for ad insertion, audience targeting, advertising, or other monetization only where Customer affirmatively enrolls in the applicable monetization feature or an applicable Order Document or Service Terms expressly authorizes that use. Libsyn acts as an Independent Controller to the extent it determines purposes and essential means for operating its advertising marketplace, selecting or measuring advertising, preventing Invalid Activity, administering payments, complying with platform requirements, or protecting the integrity of the advertising ecosystem.

For clarity, Libsyn may collect and transmit certain listener Personal Data (e.g., IP address, hashed email, mobile advertising IDs, etc.) to third parties for purposes of serving targeted advertising. Such third parties act as Independent Controller or a Third Party or Business. This transmission of this Personal Data may constitute a “Sale” (transfer for value) and/or “Sharing” (transfer for cross-context behavioral advertising) under applicable US state privacy laws. Individuals can opt out of the “sale” or “sharing” of this Personal Data as described in the Libsyn Privacy Policy (at: <https://libsyn.com/tos-policies/privacy-policy/>).

If an Order Document expressly states that Libsyn Processes specified campaign data solely on Customer’s behalf, that specified Processing is governed by Section 3 and Schedule 1 instead and Libsyn acts as a Processor.

4.5 Account and Business-Relationship Data. Libsyn acts as an Independent Controller for Customer business contact details, account-administration data, transaction records, payment and tax information, customer-service records, authentication data, and service-usage telemetry that it needs to manage the customer relationship, administer accounts, collect fees, secure the Services, comply with law, enforce the Agreement, and maintain business records.

4.6 Independent Compliance. Each party will independently comply with Applicable Data Protection Law when it acts as a Processor, including providing required notices, establishing a lawful basis, honoring applicable Data Subject rights, maintaining required records, and implementing appropriate security. Each party is responsible for the substance and timing of its own notices and responses. For clarity, the parties are not considered joint Controllers solely because data flows between them or because their respective services are technically integrated.

4.7 Controller-to-Controller Disclosures. Where one party discloses Personal Data to the other for the recipient’s independent purposes, the recipient will: (a) use the Personal Data only for the purposes described in the Agreement, this DPA, and its applicable privacy notice, if any; (b) protect it with appropriate technical and organizational security measures; (c) not Sell or Share it for cross-context behavioral advertising except as authorized by the disclosing party, the Data Subject, or Applicable Data Protection Law; and (d) provide reasonable cooperation regarding Data Subject requests or regulatory inquiries where the disclosing party cannot reasonably address the matter without the recipient’s assistance. Neither party is required to disclose its privileged or confidential information, trade secrets, information that would compromise security, or Personal Data of other persons.

4.8 Requests Concerning Libsyn Controller Data. If Customer receives a request that principally concerns Libsyn Controller Data or Libsyn's independent Processing, Customer may direct the requester to Libsyn to respond. If Libsyn receives a request that principally concerns Customer's independent Processing, Libsyn may direct the requester to Customer to respond. Each party will provide reasonable information needed to identify the responsible party, subject to verification, confidentiality, security, and law.

4.9 Personal Data Breach. Each Party, acting as an Independent Controller, shall notify the other Party in writing without undue delay after becoming aware of any actual or suspected Personal Data Breach affecting Customer Personal Data processed under this Agreement. Such notification shall include, to the extent reasonably available: (1) a description of the nature of the breach; (2) the categories and approximate number of data subjects and records concerned; (3) the likely consequences of the breach; and (4) the measures taken or proposed to be taken to mitigate or address the breach. Each party shall reasonably cooperate with and assist the other party in investigating, mitigating, and fulfilling any legal or regulatory reporting obligations relating to such Personal Data Breach.

5. DATA LIMITATIONS

5.1 Special Categories and Sensitive Data. Customer will not provide or instruct Libsyn to Process genetic data, biometric data used for unique identification, precise geolocation, government identification numbers, account credentials for third-party financial accounts, protected health information subject to HIPAA, or other special-category or sensitive Personal Data, unless the applicable Services expressly support that data and the parties authorize the Processing in an Order Document or other written agreement. Customer will not use the Services to infer sensitive characteristics unless expressly authorized in writing.

5.2 Children. Customer will not knowingly provide Personal Data of a child under 13 (in the United States) or under 16 (in the EEA or UK) or instruct Libsyn to collect such data unless the parties have expressly agreed in writing to a Service designed for that Processing and Customer has satisfied all applicable parental-consent and notice requirements. Customer is responsible for age-gating or other child-directed compliance obligations arising from Customer Content or Customer's audience practices.

5.3 Content Responsibility. Customer is solely responsible for reviewing Customer Content and metadata for Personal Data and for determining whether public distribution is appropriate. Publicly publishing Customer Content or distributing it to a Third-Party Platform may make embedded Personal Data available to the public or to third parties outside Libsyn's control.

6. SUB-PROCESSORS

6.1 General Authorization. Customer provides its general authorization to Libsyn to engage Sub-processors to Process Customer Personal Data. Sub-processors may include providers of cloud infrastructure, content delivery, data storage, communications, customer support, payment processing, security, and other technology or operational services used to provide the Processor Activities.

6.2 Sub-processor Terms and Liability. Libsyn will enter into a written agreement with each Sub-processor that imposes data-protection obligations appropriate to the Processing and are no less protective in substance than the obligations imposed on Libsyn under this DPA. Libsyn remains responsible for the Sub-processor's performance of those obligations to the extent required by Applicable Data Protection Law, subject to the limitations and exclusions of liability in the Agreement.

6.3 List and Notice. Libsyn's list of approved Sub-processors is set forth in Schedule 4. Libsyn will provide notice of a new Sub-processor by updating that list, in-product notice, email, or another reasonable means at least 30 days before the Sub-processor begins Processing Customer Personal Data, except where an emergency involving availability, security, law, or third-party service continuity requires shorter notice.

6.4 Objections. Customer may object to a new Sub-processor within ten (10) days after notice, solely on reasonable data-protection grounds. The parties will work in good faith to address the objection. If Libsyn cannot provide a commercially reasonable alternative, such as by identifying another Sub-processor acceptable to Customer, Customer may terminate the affected Processor Service by written notice before the new Sub-processor begins Processing, and Libsyn will refund any prepaid and unused fees for the terminated portion covering the period after termination. This termination right is Customer's sole remedy for an unresolved Sub-processor objection.

7. SECURITY

7.1 Security Program. Taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of Processing, as well as the risk to individuals, Libsyn will maintain appropriate technical and organizational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The measures will include the controls described in Schedule 3, as applicable to the Services and Processing.

7.2 Changes to Measures. Libsyn may update its security measures as technologies, risks, and Services evolve, provided that the updates do not materially decrease the overall protection of Customer Personal Data during the term of the Agreement.

7.3 Customer Security. Customer is responsible for securely configuring and using the Services, protecting its credentials and systems, managing user permissions, applying available security controls, and promptly notifying Libsyn of suspected account compromise. Customer will not conduct penetration tests, vulnerability scans, or other security testing of the Services without Libsyn's prior written authorization.

8. PERSONAL DATA BREACHES

8.1 Notice. Libsyn will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data. Notice does not constitute an admission of fault or liability.

8.2 Information and Cooperation. To the extent then known and reasonably available, Libsyn's notice will describe the nature of the Personal Data Breach, categories of affected Data Subjects and Customer Personal Data, likely consequences, measures taken or proposed, and a contact point. Libsyn may provide information in phases as its investigation proceeds and more information is available. Libsyn will take reasonable steps to contain, investigate, and mitigate the Personal Data Breach and will provide reasonable cooperation needed for Customer to satisfy applicable notification obligations.

8.3 Customer Communications or Notices. Customer is solely responsible for determining whether to notify Data Subjects, Supervisory Authorities, customers, or other persons and for the content of those notices. Libsyn will provide Customer with reasonable cooperation and assistance necessary for Customer to comply with its obligations under Applicable Data Protection Law with respect to notifying the relevant Supervisory Authority and/or Data Subjects affected by the Personal Data Breach.

9. DATA SUBJECT REQUESTS AND ASSISTANCE

9.1 Assistance. Libsyn shall, to the extent permitted by law, and except where Libsyn is acting an Independent Controller, notify Customer upon receipt of a request by a Data Subject to exercise any of the their rights under Applicable Data Protection Law (“**Data Subject Request**”). If Libsyn receives a Data Subject Request in relation to Customer Personal Data, Libsyn will advise the Data Subject to submit their request to Customer and Customer will be responsible for responding to such request. Customer is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of processing, or withdrawal of consent to Processing of any Personal Data are communicated to Libsyn.

9.2 Direct Requests. If Libsyn receives a request from a Data Subject concerning Customer Personal Data, Libsyn will, unless legally prohibited, direct the requester to Customer or notify Customer. Libsyn will not independently respond on Customer’s behalf unless Customer instructs Libsyn to do so or law requires a response. Libsyn may verify the requester’s identity and may respond to the extent the request also concerns Libsyn Controller Data.

9.3 Assessments and Consultations. Taking into account the nature of Processing and information available to Libsyn, Libsyn will provide reasonable assistance with Customer’s data-protection impact assessments and prior consultations that specifically relate to its Processing of Customer Personal Data.

9.4 Government and Legal Requests. Unless legally prohibited, Libsyn shall give Customer reasonable notice of a demand from law enforcement, governmental or other legal authority to disclose Customer Personal Data and cooperate to allow Customer to seek a protective order or other appropriate remedy. Libsyn shall only disclose Customer Personal Data to any law enforcement or government agency if legally obligated to do so after Libsyn has made commercially reasonable efforts to challenge the relevant disclosure request and shall only disclose the minimum amount of Customer Personal Data necessary to comply with such request.

10. AUDITS AND COMPLIANCE INFORMATION

10.1 Information. Libsyn will make available information reasonably necessary to demonstrate compliance with its Processor obligations under this DPA, which may include security summaries, questionnaires, certifications, or independent assessment reports then available for the relevant Services and completed or conducted within the previous 12 months. Customer will treat that information as Libsyn Confidential Information.

10.2 Audit Procedure. If the information under Section 10.1 is insufficient to demonstrate compliance with a specific obligation, Customer may request an audit no more than once in any rolling 12-month period, except following a Personal Data Breach affecting Customer Personal Data or where a Supervisory Authority requires an additional audit. Audits must be conducted during regular business hours, on at least 30 days' prior written notice, without unreasonable disruption to Libsyn's regular business activities, and by Customer or an independent auditor that is not a Libsyn competitor and is bound by confidentiality obligations. Audits must be limited to systems and records relevant to Customer Personal Data and may not expose information concerning other customers, security-sensitive information, or privileged material.

10.3 Costs and Reports. Customer will bear its audit costs and reimburse Libsyn's reasonable costs of supporting an audit, unless the audit identifies a material breach by Libsyn. Customer will promptly provide Libsyn a copy of the audit report, and the parties will work in good faith on a reasonable remediation plan for substantiated findings. No audit permits access to production systems, source code, penetration test details, or facilities where access would create a material security risk.

11. RETURN, DELETION, AND RETENTION

11.1 During the Term. Customer may access, export, correct, or delete Customer Personal Data using available Service functionality, subject to the Agreement and technical limitations of the applicable Service.

11.2 After Termination. Following termination or expiration of the applicable Processor Service, Libsyn will delete or return Customer Personal Data in accordance with the Agreement, Customer's written request, and Libsyn's standard retention cycle, unless Applicable Data Protection Law requires retention. Unless a different period is stated in the Agreement or applicable Service Terms, Libsyn will initiate deletion of active Customer Personal Data within 30 days after termination and will delete remaining backup copies in accordance with its ordinary backup-rotation schedule.

11.3 Retained Data. Libsyn may retain Customer Personal Data to the extent required by law or preserved in secure backups, archives, legal holds, fraud-prevention records, or business-continuity systems, provided that Libsyn continues to protect the retained data and does not actively Process it except for the purpose requiring retention or to maintain security and continuity. This Section does not require deletion of Libsyn Controller Data or Aggregated and Deidentified Data.

12. RESTRICTED TRANSFERS

12.1 Transfer Compliance. Each party will comply with Applicable Data Protection Law governing its Restricted Transfers. The transfer mechanisms in this Section apply only where required by Applicable Data Protection Law and only to the relevant role and data flows.

12.2 Processor Transfers—EU SCC Module Two. For a Restricted Transfer of Customer Personal Data from the EEA to Libsyn in a country not recognized as providing adequate protection, the EU SCCs are incorporated by reference and apply as follows: (a) Module Two (Controller to Processor) applies; (b) Customer is the data exporter; (c) Libsyn is the data importer; (d) Clause 7 (docking) does not apply; (e) in Clause 9, Option 2 and the notice period in Section 6.3 apply; (f) in Clause 11, the optional language does not apply; (g) in Clause 17, Option 1 applies and the law of Ireland governs; (h) in Clause 18(b), the courts of Ireland have jurisdiction; and (i) Schedules 1, 3, and 4 complete Annexes I–III. If Customer is a Processor exporting to Libsyn as a Sub-processor, Module Three applies to the extent legally required, and Customer represents that it has the Controller’s authorization.

12.3 Controller Transfers—EU SCC Module One. For a Restricted Transfer of Libsyn Controller Data from the EEA to Libsyn in a country not recognized as providing adequate protection, the EU SCCs are incorporated by reference and Module One (Controller to Controller) applies as follows: (a) the party disclosing the Personal Data is the data exporter; (b) the recipient is the data importer; (c) Clause 7 does not apply; (d) Clause 11’s optional language does not apply; (e) in Clause 17, Option 1, Irish law governs; (f) in Clause 18(b) the courts of Ireland have jurisdiction; and (g) Schedules 2, 3, and 4 complete the relevant annexes.

12.4 United Kingdom. For a Restricted Transfer subject to the UK GDPR, the UK Addendum is incorporated and applies to the applicable EU SCC module. The information in this DPA and its Schedules completes the tables of the UK Addendum; either party may end the UK Addendum as permitted by its mandatory termination provision; and the laws and courts of England and Wales govern the UK Addendum to the extent it requires a selection. The competent Supervisory Authority is the UK’s Information Commissioner’s Office.

12.5 Switzerland. For a Restricted Transfer subject to Swiss data-protection law, references in the EU SCCs to the GDPR include the Swiss Federal Act on Data Protection as applicable; references to the EU, EEA, and Member State include Switzerland; the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner where required; and Data Subjects in Switzerland may enforce the EU SCCs in Switzerland. The governing-law and forum selections in the EU SCCs apply without limiting mandatory Swiss rights.

12.6 Alternative Mechanism. If Libsyn adopts another valid transfer mechanism applicable to a Restricted Transfer, including an adequacy framework or certification recognized by the competent authority, that mechanism may apply instead of or in addition to the contractual mechanisms above. If a transfer mechanism becomes invalid, the parties will cooperate in good faith to implement a valid replacement.

12.7 Transfer Assessments. Upon reasonable request, Libsyn will provide information reasonably available to assist Customer in evaluating a Restricted Transfer of Customer Personal Data. Each party is responsible for its own transfer assessment and will implement supplementary measures where legally required and reasonably appropriate to the Processing.

13. THIRD-PARTY PLATFORMS

13.1 Customer Direction. If Customer enables distribution to a Third-Party Platform, Customer instructs and authorizes Libsyn to provide Customer Content, feeds, metadata, artwork, transcripts, listener-facing materials, and related data to that Third-Party Platform and to perform operational acts reasonably necessary to enable the distribution and satisfy applicable technical requirements. Libsyn acts as Customer's Processor for the transmission of Customer Personal Data to the selected Third-Party Platform.

13.2 Recipient's Role. After a Third-Party Platform receives data, that platform may Process the data as an independent Controller under its own terms and privacy notice. Customer is responsible for selecting the Third-Party Platform, accepting any separate terms, establishing a lawful basis for the disclosure, and configuring the integration. Libsyn is not responsible for the Third-Party Platform's independent Processing, security, availability, removal or restriction of Customer Content, or other action outside Libsyn's control.

13.3 Credentials and Revocation. Customer will protect credentials used for Third-Party Platform integrations and promptly disable an integration it no longer authorizes. Revoking an integration stops future transmissions within a commercially reasonable period but may not cause the Third-Party Platform to delete data previously received.

14. AI FEATURES.

To the extent Libsyn makes available any artificial intelligence, machine-learning, or similar functionality as part of the Services ("AI Features"), any Personal Information included in Customer's prompts, inputs, configurations, or other materials submitted to an AI Feature ("AI Inputs"), or contained in responses, recommendations, analyses, or other results generated by an AI Feature ("AI Outputs"), shall constitute Customer Personal Information and remain subject to this DPA.

15. LIABILITY; TERM; GENERAL

15.1 Liability. Each party's liability arising out of or relating to this DPA, the EU SCCs, or the UK Addendum is subject to the exclusions and limitations of liability in the Agreement to the maximum extent permitted by Applicable Data Protection Law. Nothing in this Section limits a Data Subject's rights under the EU SCCs or other rights that cannot lawfully be limited.

15.2 Term. This DPA remains in effect while Libsyn Processes Customer Personal Data or the parties Process Libsyn Controller Data under the Agreement. Provisions that by their nature should survive, including confidentiality, security for retained data, Restricted Transfers, liability, and deletion obligations, survive termination.

15.3 Changes Required by Law. Libsyn may update this DPA where reasonably necessary to reflect changes in Applicable Data Protection Law, regulatory guidance, transfer mechanisms, or the Services, provided that an update does not materially reduce the overall protection of Customer Personal Data. Libsyn will provide notice of material updates as required by the Agreement or Applicable Data Protection Law.

15.4 No Third-Party Beneficiaries. Except for rights expressly granted to Data Subjects under the EU SCCs, UK Addendum, or mandatory law, this DPA creates no third-party beneficiary rights.

15.5 Electronic Acceptance; Counterparts. This DPA may be accepted electronically and executed in counterparts. If the Agreement incorporates this DPA by reference or Customer accepts it through the Libsyn Platform, no separate signature is required.

SCHEDULE 1

PROCESSOR ACTIVITIES AND DETAILS OF PROCESSING

- A. Subject Matter.** Libsyn's Processing of Customer Personal Data on Customer's behalf to provide the Services selected, configured, or used by Customer under the Agreement.
- B. Duration.** For the term of the applicable Processor Activities and the deletion or retention periods described in Section 11.
- C. Nature and Purposes.** Hosting, storage, caching, encoding, transcoding, technical modification, publishing, distribution, transmission, delivery, customer-configured subscription or premium-content administration, customer support, account permissions, Customer-requested reporting, and transfer to Customer-selected Third-Party Platforms. Processing may include collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, alignment, restriction, deletion, and destruction.
- D. Processor Activities.** Processor activities include technical handling and delivery of Customer Content at Customer's direction. Under Distribution to Third-Party Platforms, Processor activities include transmitting Customer Content and related Customer Personal Data to a platform selected or enabled by Customer. Under Analytics, Advertising, and Product Improvement rights, Processor activities are limited to analytics, attribution, campaign administration, or similar work that an Order Document expressly states Libsyn performs solely on Customer's behalf. Independent uses under those licenses are listed in Schedule 2.
- E. Categories of Data Subjects.** Customer's personnel and authorized users; podcast hosts, producers, guests, contributors, and talent; subscribers and premium-content users; individuals who submit information through Customer-configured forms, support channels, or audience features; advertising contacts or campaign participants whose data Customer provides; and other individuals whose Personal Data Customer includes in Customer Content or submits to the Processor Activities.
- F. Categories of Customer Personal Data.** Names; aliases; usernames; email addresses; postal or billing contact information; customer or subscriber identifiers; account roles and permissions; authentication records; subscription status; transaction and entitlement records; support communications; information in Customer-provided lists; advertising creative and campaign data; podcast metadata, transcripts, audio, video, images, attachments, and other Personal Data contained in Customer Content; and technical data that Libsyn Processes solely to perform Customer's instructions.
- G. Sensitive Data.** None intended or permitted unless expressly authorized under Section 5. If authorized, the applicable Order Document must identify the data, Data Subjects, safeguards, and purpose.
- H. Frequency.** Continuous or intermittent, depending on Customer's use and configuration of the Services.
- I. Customer Instructions.** The Agreement, this DPA, applicable Order Documents and Service Terms, Customer's settings and enabled integrations, support requests, and other documented instructions accepted by Libsyn.
- J. Return and Deletion.** As described in Section 11 and the Agreement.

SCHEDULE 2

INDEPENDENT CONTROLLER ACTIVITIES

- A. Customer Account and Relationship Administration.** Data Subjects: Customer personnel, users, payors, and business contacts. Personal Data: names, business contact details, account identifiers, permissions, transaction records, billing and tax data, support records, and communications. Purposes: contract administration, billing, collections, customer service, records management, service communications, and legal compliance.
- B. Platform, Network, and Content Security.** Data Subjects: Customer users, listeners, visitors, suspected malicious actors, and persons connected with reported content or activity. Personal Data: IP addresses, request headers, timestamps, user agents, device or browser data, authentication events, security logs, content identifiers, and investigation records. Purposes: authentication, access control, platform integrity, abuse and fraud prevention, bot and Invalid Activity detection, incident response, enforcement, and protection of persons and property.
- C. Delivery Measurement and Analytics.** Data Subjects: listeners and users interacting with hosted or distributed content. Personal Data: IP address, timestamp, user agent, request and response data, referrer or source information, content and feed identifiers, coarse location derived from IP, event data, and measurement classifications. Purposes: counting and filtering downloads or streams, attribution, audience measurement, reporting, service quality, industry-standard compliance, and creation of Aggregated and Deidentified Data. Customer is an Independent Controller for its use of reports and statistics.
- D. Product Operations and Improvement.** Data Subjects: Customer users, listeners, visitors, and other users of the Services. Personal Data: service-usage telemetry, feature interactions, error and performance logs, support signals, content and account identifiers, and Aggregated and Deidentified Data. Purposes: monitoring, debugging, capacity planning, quality assurance, development, research, analytics, and improving or supporting the Libsyn Platform and Services.
- E. Advertising and Monetization.** Applies only where Customer affirmatively enrolls or applicable Order Documents or Service Terms authorize the activity. Data Subjects: listeners, Customer personnel, advertisers, campaign contacts, and payees. Personal Data: content and campaign identifiers, delivery and interaction events, IP address and device data where permitted, coarse geolocation, advertising identifiers where enabled and lawful, payment and tax data, and privacy-related signals. Purposes: ad serving or insertion, campaign selection and administration, attribution and measurement, audience segmentation or targeting where authorized, marketplace operations, payment, fraud prevention, and compliance.
- F. Legal, Regulatory, and Contractual Compliance.** Data Subjects: persons whose data is relevant to a legal obligation, dispute, claim, investigation, or platform requirement. Personal Data: relevant account, content, transaction, usage, security, and communication records. Purposes: responding to lawful process, enforcing agreements, establishing or defending legal claims, tax and accounting, sanctions and fraud screening, and compliance with law or Third-Party Platform requirements.
- G. Legal Bases and Retention.** Libsyn determines and documents the applicable legal basis for its Independent Controller Processing, which may include performance of a contract, legitimate interests, consent, or legal obligation, as applicable. Libsyn retains Libsyn Controller Data for periods

reasonably necessary for the relevant purpose, legal requirements, dispute resolution, security, fraud prevention, and records management, considering data sensitivity and risk.

SCHEDULE 3

TECHNICAL AND ORGANIZATIONAL MEASURES

Libsyn has implemented the following minimum technical and organizational security measures:

- 1. Governance and Risk Management.** Written information-security policies; assigned security responsibilities; risk assessment and review processes; and privacy and security training appropriate to personnel roles.
- 2. Access Controls.** Role-based and least-privilege access; authentication controls; multi-factor authentication where appropriate; credential-management requirements; periodic access review; and prompt revocation or adjustment of access following personnel or role changes.
- 3. Encryption and Transmission Security.** Encryption or other appropriate safeguards for Customer Personal Data in transit over public networks and at rest where appropriate to the risk, Service architecture, and data type; secure key and certificate practices; and protected administrative connections.
- 4. Infrastructure and Application Security.** Secure configuration; change management; network protections; logging and monitoring; malware protection where appropriate; vulnerability identification and remediation processes; secure development practices; and controls designed to separate customer environments logically where applicable.
- 5. Availability and Resilience.** Backup and recovery procedures appropriate to the Services; redundancy and capacity management where appropriate; incident-response and business-continuity processes; and periodic testing or review of recovery capabilities.
- 6. Detection and Incident Response.** Security-event logging, monitoring, escalation procedures, incident-response plans, investigation and containment processes, and post-incident remediation appropriate to the nature of an event.
- 7. Personnel and Vendor Security.** Confidentiality obligations; background screening where permitted and appropriate; security awareness; vendor due diligence; contractual security and privacy requirements; and risk-based monitoring of relevant service providers.
- 8. Data Management.** Data minimization where appropriate; retention and deletion processes; secure disposal practices; controls for production data; and deidentification or aggregation measures used for relevant analytics outputs.
- 9. Testing and Review.** Periodic assessment of the effectiveness of relevant technical and organizational measures through internal review, vulnerability assessment, independent testing, audit, or other risk-based methods.

SCHEDULE 4

EU SCC ANNEX INFORMATION

ANNEX I.A — LIST OF PARTIES

Data Exporter. Customer or the party identified in the Agreement that exports Personal Data. Address and contact details are those in the Agreement or Customer account. Activities relevant to the transfer are Customer's use of the Services and, for Module One, disclosure of Personal Data for Libsyn's independent purposes. Role: Controller for Module Two; Controller for Module One; or Processor for Module Three where applicable.

Data Importer. Liberated Syndication Inc. Address and privacy contact details are those stated in the Agreement, Libsyn's applicable privacy notice, or the Libsyn Platform. Activities relevant to the transfer are provision, security, operation, measurement, improvement, advertising, and administration of the Services as described in this DPA. Role: Controller for Module One; Processor for Module Two; or Sub-processor for Module Three where applicable.

Signature and Date. The parties' execution or electronic acceptance of the Agreement or this DPA constitutes signature of the EU SCCs on the same effective date.

ANNEX I.B — DESCRIPTION OF TRANSFER

Module One. The categories of Data Subjects, Personal Data, purposes, and activities are described in Schedule 2. Transfers may be continuous or intermittent. Retention is determined as described in Schedule 2 and Libsyn's Privacy Policy (at: XXXXXX). Sensitive data is not intended unless lawfully collected and specifically necessary for an authorized advertising, payment, security, or compliance function, in which case access limitation, encryption or equivalent safeguards, and retention controls appropriate to the attendant risk apply.

Module Two / Module Three. The categories of Data Subjects, Personal Data, sensitive data, frequency, nature, purposes, and duration are described in Schedule 1. Transfers are continuous or intermittent depending on Customer's use. The subject matter is provision of the Processor Activities. Sub-processor transfers concern cloud, delivery, storage, security, support, communications, payment, and operational services necessary to provide the Processor Activities.

ANNEX I.C — COMPETENT SUPERVISORY AUTHORITY

Competent Authority. The Supervisory Authority determined under Clause 13 of the EU SCCs. Where Customer is established in an EEA Member State, the authority for that establishment will ordinarily apply; otherwise, the authority is determined under Clause 13 based on Customer's representative or affected Data Subjects. The Irish Data Protection Commission applies only where Clause 13 validly designates it.

ANNEX II — TECHNICAL AND ORGANIZATIONAL MEASURES

The technical and organizational measures are described in Schedule 3. Their applicability and implementation depend on the relevant Service, Processing, system architecture, and risk. Libsyn may update the measures in accordance with Section 7.2.

ANNEX III — SUB-PROCESSORS

Customer provides general authorization for Sub-processors under Section 6. The categories of Sub-processors and subject matter of Processing are described in Sections 6 and Schedule 1. Libyn's list of Sub-processors is set forth below:

ID5

Adswizz

Ando Media/Triton

Barometer

Braintree

Postmark

Magellan AI

Claritas