JOINT CONTROLLERSHIP AGREEMENT

This **Joint Controllership Agreement ("JCA")** is supplementary to the **Master Platform Subscription Agreement** between **PromoRepublic Oy**, Business ID 2703642-5, a Finnish company ("**PromoRepublic**") and the entity or person(s) identified as Customer in the **Order Form** referencing this JCA (**"Customer"**).

PromoRepublic and Customer have agreed to enter into this JCA for the purposes of ensuring compliance with Data Protection Legislation.

PromoRepublic and Customer are collectively referred to as the **"Joint Controllers"** and individually referred to as a **"Joint Controller"**.

SECTION 1

PRELIMINARY PROVISIONS

1. Definitions

(a) **"Platform Subscription Agreement"** means Master Platform Subscription Agreement governing Customer's access to and use of PromoRepublic's Services.

(b) **"GDPR"** means:

(1) Regulation 2016/679 of the European Parliament and of the Council 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) (the **"EU GDPR"**);

(2) the Data Protection Act 2018 and the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the **"UK GDPR"**).

(c) **"Joint Controller"** is the natural or legal person, public authority, agency or other body which jointly with another controller, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

(d) **"International Transfer"** means:

(1) where the EU GDPR applies, a transfer of Personal Data from the European Economic Area (**"EEA"**) to a country outside the EEA which is not subject to an adequacy decision by the European Commission;

(2) where the UK GDPR applies, a transfer of Personal Data from the UK to any other country which is not based on adequacy regulations pursuant to Section 17A of the UK GDPR.

(e) **"Lawful Transfer Mechanism"** means such legally enforceable mechanism(s) for transfers of Personal Data to third countries as may be permitted under the GDPR from time to time.

(f) **"Personal Data"** means any information relating to an identified or identifiable natural person (**"Data Subject"**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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.

(g) **"Personal Data Breach"** is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

(h) **"Processing"** is any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(i) **"Standard Contractual Clauses" ("SCCs")** are 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.

(j) **"UK Addendum"** means the International Data Transfer Addendum (version B1.0) issued by the Information Commissioner's Office under s.119(A) of the UK GDPR.

(k) Any capitalized terms used but not defined in this JCA shall have the meanings given to them in the Platform Subscription Agreement and GDPR.

2. Relationship of the Joint Controllers

PromoRepublic and have agreed that they are Joint Controllers as defined in Article 26 of the GDPR as both the PromoRepublic and Customer jointly determine the purposes and means of Processing of Personal Data.

3. Scope of the JCA

(a) This JCA applies to the Processing of Personal Data in the context of the Platform Subscription Agreement, where and to extent to PromoRepublic and Customer are acting as the Joint Controllers.

(b) The joint controllership under the Platform Subscription Agreement applies only to:

(1) the initial collection and transmission of Personal Data through the Platform to Joint Controllers' systems for Processing;

(2) the subsequent Processing of such Personal Data on Joint Controllers' (or its Processors') systems as necessary in order to provide Platform Services to users;

(3) the Processing of Personal Data as necessary for the purpose of fulfilling the rights of Data Subjects in accordance with the GDPR (the **"Joint Processing"**).

(c) This JCA is limited to Personal Data related to the Platform Services under the Platform Subscription Agreement.

4. Interpretation

This JCA shall not be interpreted in a way that runs counter to the rights and obligations provided for in the GDPR or in a way that prejudices the fundamental rights or freedoms of the Data Subjects.

5. Hierarchy

(a) In the event of a contradiction between this JCA and the provisions of related agreements between the Joint Controllers existing at the time when this JCA is agreed or entered into thereafter, this JCA shall prevail.

(b) In the event of a contradiction between this JCA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

SECTION 2
JOINT CONTROLLERSHIP OBLIGATIONS

6. Retention of Data

PromoRepublic and Customer will retain the Personal Data of Data Subjects as each of them describe in their own Privacy Policies and Data Retention Policies, as applicable.

7. Main Purpose of Data Processing

(a) Processing of Personal Data will be undertaken by PromoRepublic and Customer for purposes directly related to the Platform Subscription Agreement and Platform Services.

(b) PromoRepublic and Customer each shall comply with their obligations under the GDPR when collecting, disclosing, sharing, using or otherwise processing Personal Data of Data Subjects in connection with the Platform Services, including ensuring that they have a legal basis for the Processing of Personal Data.

(c) PromoRepublic and Customer are not responsible for Processing of Personal Data for their own purposes.

8. Data Subject Rights

PromoRepublic and Customer have agreed the following procedures to allow Data Subjects to exercise these rights under the GDPR. It should be noted that the Data Subjects may exercise their rights against each of the controllers as stated in Article 26.3 of the GDPR.

8.1. Right of Accessing Personal Data

PromoRepublic will provide the Data Subject with a copy of Personal Data undergoing Processing as required under Article 15 of the GDPR.

8.2. Right of Rectification of Personal Data

The Data Subject may request the rectification of any inaccurate and/or incomplete personal data held by the joint controller under Article 16 of the GDPR. Where the personal data is provided by the Data Subject, PromoRepublic will correct any inaccurate data and make it available to the Customer.

8.3. Right of Erasure of Personal Data and Objection to the Processing of Personal Data

The Data Subject may request the erasure of Personal Data held by the joint controller under Article 17 of the GDPR. If the Data Subject makes the request, the Joint Controller will delete the data and inform the other Joint Controller of the request who

will delete any data on their system. Joint Controllers shall promptly comply with requests from the Data Subjects objecting to the Processing of their Personal Data, including opt-out of direct marketing activities.

8.4. Right of Data Portability

PromoRepublic will administer any requests for data portability under Article 20 of the GDPR. Where this request relates to processes conducted solely by the Customer or data held solely by the Customer, this request will be forwarded directly to the Customer.

8.5. Provision of Information Regarding Processing

The Joint Controllers will provide the Data Subject with information required under Articles 13 and 14 of the GDPR and post its privacy policy on the Platform in connection with the Platform Services. The Joint Controllers will make the essence of the JCA available to Data Subjects through appropriate disclosures within Privacy Policy on the Platform.

9. Security

PromoRepublic and Customer must implement appropriate technical and organizational measures listed but not limited to Annex II to ensure and to be able to demonstrate that Processing is performed in accordance with the GDPR.

10. Use of Processors and Sub-processors

(a) PromoRepublic and Customer are entitled to use other Processors and/or Sub-processors in connection with the Platform Services.

(b) If any Processors and/or Sub-processors are used, each Joint Controller is responsible for compliance with the requirements of Article 28 of the GDPR. The Joint Controller is obliged, *inter alia*, to:

(1) use only Processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subject;

(2) ensure that a valid data processing agreement has been made between the Joint Controllers and the Processor.

11. Records of Processing

Each Joint Controller is responsible for its own compliance with the requirement for records of processing activities in Article 30 of the GDPR.

12. Notification of Personal Data Breach to the Supervisory Authority

(a) Each Joint Controller is responsible for compliance with Article 33 of the GDPR on notification of the Personal Data Breach to the supervisory authority.

(b) The Joint Controller with whom a Personal Data Breach was committed or from whom the reason for the breach originates is responsible for notifying the Personal Data Breach to the supervisory authority.

(c) Immediately after having become aware of the Personal Data Breach, the Joint Controller must inform the other Joint Controller of the breach. The other Joint Controller must be kept informed of the process after the discovery of the Personal Data Breach and will receive a copy of the notification to the supervisory authority.

(d) If the reason for the breach is not immediately attributable to one of the Joint Controllers, PromoRepublic is responsible for notifying the Personal Data Breach to the supervisory authority.

13. Communication of Personal Data Breach to the Data Subject

(a) Each Joint Controller is responsible for compliance with Article 34 of the GDPR on communication of the Personal Data Breach to the Data Subject.

(b) If the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, the Joint Controller with whom the Personal Data Breach was committed, or from whom the reason for the breach originates is responsible for communicating the Personal Data Breach to the Data Subjects affected.

(c) If the reason for the Personal Data Breach is not directly attributable to one of the Joint Controllers, and the breach is likely to result in a high risk to the rights and freedoms of natural persons, PromoRepublic is responsible for communicating the Personal Data Breach to Data Subjects affected.

14. Data Protection Impact Assessment and Prior Consultation

(a) Each Joint Controller is responsible for compliance with the requirement in Article 35 of the GDPR on data protection impact assessment. Where a type of Processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of

natural persons, the Joint Controllers must, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data.

(b) The Joint Controllers are obliged to comply with the requirement in Article 36 of the GDPR on prior consultation of the supervisory authority when this is relevant.

15. International Transfers

(a) Each Joint Controller is responsible for its own International Transfers of Personal Data, including for ensuring that a legal basis for transfer exists and that Chapter V of the GDPR has been observed.

(b) Joint Controllers shall make International Transfers of Personal Data in connection with the Platform Services only where appropriate safeguards are provided, and on condition that enforceable rights and effective legal remedies for Data Subjects are available. Such international transfers are effected by way of a Lawful Transfer Mechanism, including the SCCs, UK Addendum (provided the conditions for the use of foregoing agreements are met) or a relevant contract that guarantees that Personal Data will be protected as required by the GDPR.

(c) Where the Processing involves data transfers from PromoRepublic to the Customer established in a third country, the SCCs shall be incorporated by reference and form an integral part of this JCA with PromoRepublic as **"Data exporter"** and Customer as **"Data importer"**. For the purposes of the SCCs:

(1) the Module One (Controller to Controller) provisions shall apply and the Module Two, Three and Four provisions shall be deleted in their entirety;

(2) Clause 7 shall be omitted;

(3) in Clause 11 right to lodge a complaint with an independent dispute resolution body shall not be included;

(4) for the purpose of Clause 13 the data exporter is established in an EU Member State;

(5) in Clause 17, Option 1 shall apply and the SCCs shall be governed by the law of Finland;

(6) in Clause 18 (b), disputes shall be resolved before the courts of Finland;

(7) the Annexes of the SCCs shall be populated with the information set out in the Annexes to this JCA;

(8) In the event of a contradiction between the SCCs and the provisions of related agreements between the Joint Controllers, existing at the time these SCCs are agreed or entered into thereafter, these SCCs shall prevail.

16. Complaints

(a) Each Joint Controller is responsible for the handling of any complaints from Data Subjects if the complaints relate to the infringement of provisions in the GDPR, for which the Joint Controller is responsible according to this JCA.

(b) If one of the Joint Controllers receives a complaint which should rightfully be handled by another Joint Controller, the complaint is forwarded to such Joint Controller without undue delay.

(c) If one of the Joint Controllers receives a complaint, part of which should rightfully be handled by another Joint Controller, such part is forwarded for reply by the Joint Controller without undue delay.

(d) In connection with the forwarding of a complaint or part of a complaint to another Joint Controller, the Data Subject must be notified about the essence of this JCA.

(e) The Joint Controllers shall inform each other about all complaints received about the Platform Services.

SECTION III
FINAL PROVISIONS

17. Termination of the JCA

(a) This JCA will terminate contemporaneously and automatically with the termination of the Platform Subscription Agreement.

(b) Notwithstanding the expiry or termination of this JCA for any reason the provisions of this JCA shall continue to apply to any Personal Data in the possession of either party which was covered by the JCA.

18. Jurisdiction

This JCA shall be governed by and construed in accordance with the provisions of the governing law and jurisdiction in the Platform Subscription Agreement, unless otherwise required by Data Protection Legislation.

ANNEX I

A. LIST OF PARTIES

DATA EXPORTER	DATA IMPORTER
Name: PromoRepublic Oy	**Name:** entity/ies identified as Customer in the Order Form
Company number: 2703642-5	**Company number:** the Customer's company number
Address: specified on the Order Form by PromoRepublic	**Address:** the Customer's address
Contact person's name, position and contact details: the Primary Contact name, position, email specified on the Order Form by PromoRepublic	**Contact person's name, position and contact details:** the Primary Contact name, position, email specified on the Order Form by the Customer
Activities relevant to the data processed under these Clauses: Provision of the Services in accordance with the Platform Subscription Agreement.	**Activities relevant to the data processed under these Clauses:** Customer orders and receives Services in accordance with the Platform Subscription Agreement.
Role: Controller	**Role:** Controller

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose Personal Data is transferred: Customer's Team Members/Users, employees, contractors, representatives, as well as all relevant end users of the Platform Services on behalf of the Customer.

Categories of Personal Data transferred: Personal and Business Contact information, Account information, User Content, Feedback and correspondence, Information from Connected Social Networks and Social Media Accounts, Technical Information and any other Personal Data that Data Subjects provide on or through the Platform.

The frequency of the transfer: on a continuous basis.

Nature of the Processing: any or all of the following processing operations: collection, recording, organization, structuring, storage, adaptation/alteration, retrieval, consultation, use, alignment / combination, restriction, erasure / destruction.

Purpose(s) of the data transfer and further Processing: provision and promotion of the Platform Services.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: The Personal Data shall be retained for no longer than necessary for the purpose(s) of the Platform Subscription Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

(a) With respect to the processing of Personal Data to which the GDPR applies, the competent supervisory authority is:

Office of the Data Protection Ombudsman
P.O. Box 800
FI-00531 Helsinki
Tel. +358 29 56 66700
Fax +358 29 56 66735
Email: tietosuoja@om.fi
Website: http://www.tietosuoja.fi/en/

(b) With respect to the processing of Personal Data to which the UK GDPR applies, the competent supervisory authority is:

Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF,
United Kingdom
Tel. 0303 123 1113
Fax 01625 524510
Contact details: https://ico.org.uk/global/contact-us/
Website: https://ico.org.uk/

ANNEX II

TECHNICAL AND ORGANIZATIONAL MEASURES

The Joint Controllers implement the following technical and organizational measures:

Measures of encryption of Personal Data: The Joint Controllers encrypt the Personal Data in transit and at rest. All external data transmission happens through encrypted connections.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services: The personnel working on the data processing are authorized. The Joint Controllers control that data is consistent, trustworthy and accurate. The Joint Controllers ensure that data is protected against accidental destruction or loss, and systems can continue operating under adverse conditions.

Measures for ensuring the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident: The Joint Controllers have documented incident or breach response management plans and procedures in place to ensure a quick, effective and orderly response to security incidents.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing: The Joint Controllers conduct regular vulnerability scans.

Measures for user identification and authorisation: The Joint Controllers prevent data from being accessed by unauthorized persons.

Measures for the protection of data during storage: The Joint Controllers implement data storage security policies to keep data secure.

Measures for ensuring physical security of locations at which Personal Data are processed: The Joint Controllers ensure that physical, environmental and infrastructure controls are implemented.

Measures for ensuring events logging: The Joint Controllers configure and perform the collection and analysis of security events.

Measures for internal IT and IT security governance and management: The Joint Controllers have appropriate internal security policies.

Measures for ensuring data minimisation: The Joint Controllers ensure that Personal Data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

Measures for ensuring data quality: The Joint Controllers ensure that data is complete, unique, valid, timely, and consistent through regular updates and data verification.

Measures for ensuring limited data retention: Personal Data are kept for no longer than is necessary for the purposes for which the Personal Data are processed.

Measures for ensuring accountability: The Joint Controllers are responsible for and are able to demonstrate compliance with the data processing principles.