JOINT CONTROLLER AGREEMENT

PARTIES

Firefish Limited, incorporated and registered in England and Wales with company number 03854900 whose registered office is at 170-172 Tower Bridge Road, London, SE1 3LS, UK (**Firefish**); and

[FULL COMPANY NAME] incorporated and registered in England and Wales with company number [NUMBER] whose registered office is at [REGISTERED OFFICE ADDRESS] (**Client**).

together the "**Parties**".

BACKGROUND

(A) The Parties have determined that they are Joint Controllers in relation to the Personal Data described below and accordingly this Agreement sets out the arrangements between them for the purposes of Article 26 of the GDPR and/or Article 26 of the UK GDPR, as applicable.

(B) This Agreement shall form part of the Main Agreement which incorporates the commercial arrangement and terms established by the Parties in respect of the Services.

1. Definitions and interpretation:

1.1. "**Controller**" means the Party who determines the purposes and means of processing Personal Data;

"**Data Protection Legislation**" means all laws, rules, and regulations relating to the processing of Personal Data if and as applicable to a party's performance under the Agreement, including without limitation:

(i) the UK General Data Protection Regulation which has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018) (the "**UK GDPR**")

(ii) the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and any national implementing laws, regulation(s) and secondary legislation in each case as such law(s) may be replaced, supplemented, substituted or amended from time to time;

(iii) the European Privacy and Electronic Communications Directive (Directive 2002/58/EC);

(iv) Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. § 6501 et seq;

"Data Subject" means the identified or identifiable natural person who is the subject of Personal Data;

"Joint-Controllers" means two or more parties who jointly Control Personal Data;

"Main Agreement" means the executed agreement / terms and conditions for the provision of the Services by Firefish to Client dated [ ];

"**Personal Data**" means any information relating to an identified or identifiable living individual. An identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 the individual;

"Processor" means a party who processes Personal Data on behalf of a Controller;

"**Processing**" means 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;

"**Services**" means the services to be provided to Client by Firefish under the Main Agreement;

"**Standard Contractual Clauses**" means the Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to GDPR approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj;

"**Supervisory Authority**" means an independent public authority which concerns itself with the Processing of Personal Data;

"UK Standard Contractual Clauses" means the Standard Contractual Clauses for Controller to Controller transfers of Personal Data approved by the European Commission in decision 2004/915/EU. as currently set out at:

https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF or any replacement standard contractual clauses or international data transfer agreement approved by the UK Information Commissioner's Office.

1.2 This Agreement is subject to the terms of the Main Agreement and is incorporated into the Main Agreement.

1.3 In the case of conflict or ambiguity between any of the provisions of this Agreement and the provisions of the Main Agreement, the provisions of this Agreement will prevail.

2. Purpose

2.1. The Parties agree that in respect of the Services, they jointly determine the purposes and means (within the meaning of controllership set out in GDPR) of processing the Personal Data and are therefore Joint Controllers in this respect. The relevant Personal Data is identified in Schedule 1.

2.2. The purpose of this Agreement is to set out the responsibilities of the Parties as Joint Controllers. Setting out these responsibilities and subsequently making specific arrangements that put them into effect will assist the Parties to understand their respective responsibilities and the actions they need to take to comply with the Data Protection Legislation.

3. Compliance with National Data Protection Laws

3.1. Each Party must ensure compliance with applicable Data Protection Legislation at all times during the term of this Agreement.

3.2. In the event the data protection law or approach to compliance of the UK/EEA country and any other country whose data protection law apply conflict, the requirements of the country that necessitates stricter or additional requirements to protect data subjects' privacy and Personal Data shall be applied.

4. Joint Controller Responsibilities

4.1. The Parties have set out in Schedule 2 to this Agreement who is responsible for specific Data Controller responsibilities.

4.2. The Parties shall each provide contact details for a single point of contact for the purpose of communication with regard to their respective responsibilities and shall notify each other of any changes to those details in writing without delay:

Firefish: dataprotection@firefish.ltd.uk
Client: [ ]

4.3. The Parties shall only share Personal Data with the other Party in a secure manner.

4.4. Each of the Parties shall process the Personal Data in line with the permissions gained and privacy notice provided to the Data Subject at the point of data collection.

5. Provision of Information to Data Subjects

5.1. The Parties are obliged as Data Controllers to provide certain information to the Data Subjects. In accordance with the Data Protection Legislation, the Parties have specified in Schedule 2 to this Agreement which of them is responsible for providing the relevant information in each case. The responsible Party shall ensure that this information is accessible via the Internet.

5.2. The necessary information shall be provided in a precise, transparent, comprehensive, and easily accessible form and in a clear and simple language.

5.3. Each Party shall consult with the other Party about any notices given to Data Subjects.

6. Enforcement of Data Subject Rights

6.1. The parties are obliged as Data Controllers to comply with the Data Protection Legislation regarding the exercise by Data Subjects of their rights under GDPR. Accordingly, the parties have specified in Schedule 2 which of them is responsible for responding to and fulfilling requests by Data Subjects to exercise their rights.

6.2. If both Parties are designated responsible for responding to Data Subject access requests, the Party who receives the request shall respond, with the other Party's co-operation and assistance if reasonably requested.

6.3. Notwithstanding Clause 5.1 above, the Parties acknowledge that under the Data Protection Legislation, the Data Subject may exercise his or her rights in respect of and in against each of the Parties regardless of the allocation of responsibility set out in Schedule 2. If a Party who is not primarily responsible for responding to and fulfilling Data Subject Access requests receives such a request, it shall:

(i) promptly inform the other Party and pass on the request in full;
(ii) provide the other Party with reasonable assistance in complying with the request; and
(iii) not disclose or release any Personal Data in response to a Data Subject access request without first consulting the other Party wherever possible.

7. Data Transfers

7.1. Neither Party will transfer any of the Personal Data to a country or international organisation (whether own or third party organisation) located outside the country of origin of the Personal Data unless it ensures that it complies with the obligations set out in Data Protection Legislation regarding the transfer of Personal Data to third countries or international organisations, including, for example, by the use of an approved transfer mechanism such as the Standard Contractual Clauses in the case of EEA Personal Data or the UK Standard Contractual Clauses in the case of UK Personal Data.

7.2. In the case of transfers of Personal Data between the parties where that Personal Data is governed by the GDPR ("EEA Personal Data") or the UK GDPR ("UK Personal Data") and where the importing party is located in a country outside the EEA or UK which is not recognized by the EU or the UK as providing an adequate level of protection for Personal Data, the parties hereby agree to and hereby enter into the SCCs (subject to the additional terms set out in Schedule 3) in the case of EEA Personal Data, and/or the UK SCCs in the case of UK Personal Data.

8. Data Security

8.1. The Parties shall both implement appropriate technical and organisational measures to protect the personal data, in accordance with Article 32 of GDPR.

9. Notifications, Data Breaches and Reporting Procedures

9.1. Each Party shall immediately inform the other Party of any actual Personal Data Breach within 1 business day of becoming aware of the breach. The Parties shall immediately provide each other with all information reasonably required for the examination of such Personal Data Breach and its consequences.

9.2. In the event that a Personal Data Breach must be reported to the relevant Supervisory Authority or Data Subject(s) concerned, the Parties shall coordinate further action and fully support each other in fulfilling these obligations within the required time periods under GDPR.

10. Cooperation with Supervisory Authorities

10.1. Each Party shall inform the other without undue delay if a Supervisory Authority approaches it concerning any Personal Data or processing activity covered by the Main Agreement.

10.2. The Parties shall coordinate their individual responses, or a joint response if appropriate, to enquiries from Supervisory Authorities to the extent that this is legally permissible and/or reasonable. In respect of any ongoing proceedings with Supervisory Authorities, the Parties shall keep each other fully informed and provide all reasonable co-operation, information and assistance in respect of such proceedings.

11. Resolution of Disputes with Supervisory Authorities or with Data Subject

11.1. In the event of a dispute or claim brought by a Data Subject, the Information Commissioner or by a Supervisory Authority concerning the processing of the Personal Data against either or both Parties, the Parties will inform each other about any such disputes or claims and will co-operate with a view to settling them amicably in a timely fashion.

11.2. The Parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

12. Warranties

12.1. Each of the Parties warrant that it shall:
(i) at all times in its roles at Data Controller in respect of the Personal Data comply with the applicable Data Protection Legislation;
(ii) provide reasonable assistance to the other Party in complying with all applicable requirements of the Data Protection Legislation insofar as they pertain to the Services;
(iii) maintain complete and accurate records and information to demonstrate its compliance with this Agreement.

13. Liability

13.1. Subject to Clause 13.2, the total aggregate liability of each Party for loss arising from that Party's failure to comply with its obligations under this Agreement will be limited to £1 million.

13.2. Nothing in this Agreement limits any liability which cannot legally be limited including, but not limited to, liability for death or personal injury caused by negligence and fraud or fraudulent misrepresentation.

14. Indemnity

Subject to Clause 13, each Party shall indemnity the other Party against all liabilities, costs, expenses, damages and losses (including reasonable legal costs and all other reasonable professional costs and expenses, but not including consequential losses, loss of profit or loss of reputation) suffered or incurred by the indemnified Party caused by the breach of the Data Protection Legislation or the terms of this Agreement by the indemnifying Party, its employees or agents, provided that the indemnified Party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it and reasonable assistance in dealing with the claim.

This agreement has been entered into on the date stated at the beginning of it.

Signed by [NAME OF DIRECTOR]
for and on behalf of **Firefish Limited** Director

Date

Signed by [NAME OF DIRECTOR]
for and on behalf of [NAME OF **Client**] Director

Date

Schedule 1

Personal Data Processing

Purpose of processing:

Market research services - market research recruitment, fieldwork, analysis, reporting and deliverables

Frequency of processing: processing will be ad hoc and dependent on each project as set out in any applicable research proposal

Duration of processing: duration will be as per each Party's current retention policy

Types of Personal Data:

The following types of personal data are typically subject to processing:

- Name
- Address
- Email address
- Contact telephone number/s
- Pictures
- Videos
- Audio and video recordings
- Demographic information
- Bank details for incentives paid via BACS
- Other types of personal data not listed will be subject to informed consent of the data subjects

Special Category Data:

The following types of special category data are regularly subject to processing:

- Racial or ethnic origin
- Health
- Sex Life/Sexual Orientation

Other types of special category data not listed will be subject to explicit consent of the data subjects

Categories of Data Subjects: Market research participants

Competent Supervisory Authority: Information Commissioner's Office, U.K.

Technical and Organisational Measures:

The Parties shall ensure that Personal Data is Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. To this end, the Parties shall implement and maintain a security program and security measures that are aligned to ISO/IEC 27001:2013, NIST or equivalent industry standard security controls. At a minimum, the following security measures shall be implemented:

- Measures of pseudonymisation and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring data minimisation
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for ensuring accountability

Schedule 2

Distribution of Responsibilities

Responsibility	Responsible Party
Decision to undertake and commission research	Client
Collection of personal data at source and processing during research fieldwork	Firefish
Ensuring legal basis of personal data collection	Firefish
Providing privacy notice	Firefish
Determine who will be contacted i.e. target audience	Firefish and Client
Deciding purpose/purposes personal data will be used for	Firefish and Client
Items of personal data to be collected	Firefish and Client
Decision to disclose personal data and to who	Firefish and Client
Data retention	Firefish and Client
Responding to Data subject access requests/DPO queries	Firefish and Client
Reporting data breach to supervisory authority	Firefish and Client
Responding to supervisory authority requests	Firefish and Client depending on scenario - refer to clause 8.2

Appendix 3 – Standard Contractual Clauses: Additional Terms

1. For the purposes of any transfers made under the SCCs in accordance with the relevant clause/s in this Joint Controller Agreement, the parties shall comply with the terms of the Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent that they reference Module One (Controller to Controller), subject to the terms of Section 2 below.

2. Standard Contractual Clauses – Operative Provisions and Additional terms. For the purposes of this Section 2 and Section 3 below only, all further reference to "clauses" are references to the relevant sections of the Standard Contractual Clauses;

   (a) The relevant provisions of the Standard Contractual Clauses are hereby incorporated by reference and are an integral part of this Joint Controller Agreement;

   (b) Docking Clause. The option under clause 7 shall not apply;

   (c) General Authorisation for use of Sub-processors. Option 2 under clause 9 shall apply. The time period for prior notice of sub-processor changes will be thirty (30) days unless otherwise agreed in writing between the parties;

   (d) Redress. The option under clause 11 shall not apply;

   (e) Governing Law. The governing law for the purposes of clause 17 shall be the law governing the Main Agreement;

   (f) Choice of forum and jurisdiction. The courts under clause 18 shall be those designated in the Main Agreement;

   (g) Annexes. In Annex I, the details of the parties are as set out in this Agreement. The remaining information in Annex I and Annex II is as set out in Schedule 1 to this Agreement.

3. The Parties agree that the Data Subjects whose Personal Data transferred under this Agreement are third-party beneficiaries under the Standard Contractual Clauses.

4. Conflict. In the event of any conflict or inconsistency between the body of this Agreement or the Main Agreement on the one hand, and the Standard Contractual Clauses on the other, the Standard Contractual Clauses shall prevail.

5. By entering into this Agreement, the parties are deemed to have signed the SCCs including their Annexes as of the Effective Date of the Agreement.