DATA PROTECTION ADDENDUM

This Data Processing Addendum ("DPA") forms an integral part of the main agreement ("Agreement") between EX.CO Technologies Ltd. ("Company") and between the counterparty to that Agreement ("Customer"; each a "Party" and together the "Parties") and applies to the extent that Company processes Personal Data in the course of its performance of its obligations under the Main Agreement.

If you are accepting this DPA on behalf of Customer, you warrant that: (a) you have full legal authority to bind Customer to this DPA; (b) you have read and understand this DPA; and (c) you agree, on behalf of Customer, to this DPA. If you do not have the legal authority to bind Customer, please do not accept this DPA.

1. Introduction
1.1 This DPA reflect the parties’ agreement on the processing of Personal Data in connection with the Data Protection Laws.
1.2 Any ambiguity in this DPA shall be resolved to permit the parties to comply with all Data Protection Laws.
1.3 In the event and to the extent that the Data Protection Laws impose stricter obligations on the parties than under this DPA, the Data Protection Laws shall prevail.

2. Definitions and Interpretation
2.1 In this DPA:
   (a) "Affiliate" means an entity that directly or indirectly controls, is controlled by, or is under common control with, a Party.
   (b) "Approved Jurisdiction" means a member state of the European Economic Area, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
   (c) "Data Protection Laws" means, any and all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state, federal or national level, pertaining to data privacy, data security or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (as amended, and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"), the Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"), the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. and the regulation enacted thereunder ("CCPA"); the Virginia Consumer Data Protection Act, Va. Civ. Code § 59.1 ("VCDPA") (the CCPA and the
VCDPA are hereinafter collectively referred to as "US Data Protection Laws"; and any amendments or replacements to the foregoing.

(d) “Data Subject” means an individual to whom Personal Data relates.

(e) “Personal Data” means any personal data (as this terms is defined under the GDPR) that is processed by a Party under the Agreement in connection with its provision or use (as applicable) of the services for which the parties agreed to in the Agreement.

(f) "Security Incident" shall mean any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. For the avoidance of doubt, any Personal Data Breach will comprise a Security Incident

(g) “Standard Contractual Clauses” means (a) where the GDPR applies - the applicable Module (Modules One or Four, as applicable) of the 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 from June 4th 2021, as available here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en; and (b) with respect to data transfers to which the UK GDPR applies - the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, which was entered into force on 21 March, 2022, as available here: https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf; both (a) or (b) above, as applicable, are incorporated herein by reference.

(h) The terms “controller”, “processing” and “processor” as used in this DPA have the meanings given to them in Data Protection Laws. Where applicable, a controller shall be deemed a “Business” and a processor shall be deemed a “Service Provider” or a "Contractor", as these terms are defined under US Privacy Laws.

(i) Any reference to a legal framework, statute or other legislative enactment is a reference to it as amended or re-enacted from time to time.

3. Application of this DPA

3.1 This DPA will only apply to the extent all of the following conditions are met:

3.1.1 Company processes Personal Data that is made available by the Customer in connection with the Agreement;

3.1.2 The Data Protection Laws applies to the processing of Personal Data.

3.2 This DPA will only apply to the services for which the parties agreed to in the Agreement, which incorporates the DPA by reference.

4. Roles and Restrictions on Processing

4.1 Independent Controllers. Each Party:

(a) is an independent controller of Personal Data under the Data Protection Laws;

(b) will individually determine the purposes and means of its processing of Personal Data; and

(c) will comply with the obligations applicable to it under the Data Protection Laws with respect to the processing of Personal Data.

4.2 Restrictions on Processing. Section 4.1 (Independent Controllers) will not affect any restrictions on either Party’s rights to use or otherwise process Personal Data under the Agreement.
4.3 **Sharing of Personal Data.** In performing its obligations under the Agreement, a Party may provide Personal Data to the other Party. Each Party shall process Personal Data only for (i) the purposes set forth in the Agreement or as (ii) otherwise agreed to in writing by the parties, provided such processing strictly complies with (iii) Data Protection Laws, (ii) Relevant Privacy Requirements and (iii) its obligations under this Agreement (the "Permitted Purposes"). Each Party shall not share any Personal Data with the other Party (i) that allows Data Subjects to be directly identified (for example by reference to their name and e-mail address); (ii) that contains Personal Data relating to minors.

4.4 **Lawful grounds and transparency.**

4.4.1 Each Party shall maintain a publicly-accessible privacy policy on its mobile apps and websites that is available via a prominent link that satisfies transparency disclosure requirements of Data Protection Laws.

4.4.2 It is hereby clarified that Customer is the initial Controller of Personal Data. Customer acknowledges that Company and its advertisers use cookies and similar tracking technologies in order to provide the services under the Agreement, including for the purpose of cross-site or cross-device advertising. Customer warrants and represents that it has provided Data Subjects with appropriate transparency and all required notices regarding personal data processing, transfer, implementation of tracking technologies (including where applicable, by Company and demand partners), and obtained any and all consents or permissions necessary under Data Protection Laws with respect thereto. Where Customer relies on consent as its legal basis to Process Personal Data, it shall ensure that it obtains a proper affirmative, specific and unambiguous consent from Data Subjects in accordance with Data Protection Laws.

4.4.3 Both parties will cooperate in good faith in order to identify the information disclosure requirements and each Party hereby permits the other Party to identify it in the other Party’s privacy policy, and to provide a link to the other Party’s privacy policy in its privacy policy.

4.5 **Data Subject Rights.** It is agreed that where either Party receives a request from a Data Subject in respect of Personal Data controlled by such Party, then such Party shall be responsible to exercise the request, in accordance with Data Protection Laws.

5. **Personal Data Transfers**

5.1 **Transfers of Personal Data Out of the European Economic Area.** Either Party may transfer Personal Data outside the European Economic Area if it complies with the provisions on the transfer of personal data to third countries in the Data Protection Laws (such as where the transfer of Personal Data is to an Approved Jurisdictions or through the use of Standard Contractual Clauses, or other applicable frameworks).

5.2 To the extent that Company processes Personal Data outside the EEA or an Approved Jurisdiction, then the Parties shall be deemed to enter into the Standard Contractual Clauses, subject to any amendments contained in Schedule A, in which event: (i) the Standard Contractual Clauses are incorporated herein by reference; and (ii) the Customer shall be deemed the data exporter and the Company shall be deemed the data importer (as these terms are defined therein).

6. **Protection of Personal Data.**

6.1 The Parties will provide a level of protection for Personal Data that is at least equivalent to that required under Data Protection Laws. Both Parties shall implement appropriate technical and organizational measures to protect the Personal Data. In the event that a Party suffers a
confirmed Security Incident, each Party shall notify the other Party without undue delay and the Parties shall cooperate in good faith to agree and action such measures as may be necessary to mitigate or remedy the effects of the Security Incident.

7. Liability
7.1 Notwithstanding anything else in the Agreement, the total liability of either Party towards the other Party under or in connection with this DPA will be limited to the maximum monetary or payment-based amount at which that Party’s liability is capped under the Agreement (for clarity, any exclusion of indemnification claims from the Agreement’s limitation of liability will not apply to indemnification claims under the Agreement relating to the Data Protection Laws).

8. Priority
8.1 Effect of this DPA. If there is any conflict or inconsistency between the terms of this DPA and the remainder of the Agreement then, the terms of this DPA will govern. Subject to the amendments in this DPA, the Agreement remains in full force and effect.

9. Changes to this DPA.
9.1 Company may change this DPA if the change is required to comply with Data Protection Laws, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Parties as independent controllers of Personal Data under the Data Protection Laws; (ii) expand the scope of, or remove any restrictions on, either Party’s rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.
9.2 Notification of Changes. If Company intends to change this DPA under this Section, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

The parties acknowledge that they have read and understood the terms of this DPA and agree to be legally bound by it.
Schedule A – SCC

1. If Customer is a controller – the Parties shall be deemed to enter into the Controller-to-
Controller Standard Contractual Clauses (Module One); if Customer is a processor – the
Parties shall be deemed to enter into the Processor to Controller Standard Contractual
Clauses (Module Four).

2. This Schedule A sets out the Parties’ agreed interpretation of their respective obligations
under the Standard Contractual Clauses.

3. The Parties agree that for the purpose of transfer of Personal Data between the Company
(Data Exporter) and the Recipient (Data Importer), the following shall apply:

   3.1. Clause 7 of the Standard Contractual Clauses shall not be applicable.

   3.2. In Clause 11, data subjects shall not be able to lodge a complaint with an independent
dispute resolution body.

   3.3. In Clause 11, data subjects shall not be able to lodge a complaint with an independent
dispute resolution body.

   3.4. In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by
the law of the state of Ireland.

   3.5. In Clause 18(b) the Parties choose the courts of Dublin.

4. To the extent the UK GDPR applies, the following shall apply as well:

   4.1. All the information provided under the Standard Contractual Clauses shall apply to the
UK Addendum with the necessary changes per the requirement of the UK Addendum. Annexes
1A, 1B and 2 to the UK Addendum shall be replaced with the Annexes below, respectively.

   4.2. In Table 4 of the UK Addendum, either party may terminate the agreement in accordance
with section 19 of the UK Addendum.

5. The Parties shall complete Annexes I–II below, which are incorporated in the Standard
Contractual Clauses by reference.
Annex I – Description of processing activities

A. Identification of Parties

"Data Exporter": Customer;

"Data Importer": Company.

B. Description of Transfer

Data Subjects

The Personal Data transferred concern the following categories of Data Subjects (please specify):

- End users who use or interact with Embedded Items through Customer's properties.
- Customer's personnel who use or interact with the Services.

Categories of Personal Data

The Personal Data transferred concern the following categories of data (please specify):

- IP address, cookie IDs, unique device identifiers
- Location (non-precise)
- Interactions with Embedded Items (e.g., clicks, timestamps) insofar as such actions amount to being Personal Data
- Contact data (e.g., names, email addresses) solely to the extent Customer opts to collect and share such data with Company (for example in the context of Customer's implementation of polls, surveys, or similar forms)

Special Categories of Data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

None
The frequency of the transfer

The frequency of the transfer:

Continuous

Nature of the processing

Processing shall be carried out by Company on order to provide the Services to Customer, as set out in the Main Agreement. Such processing may include the collection, recording, organization or structuring, storage, adaptation or alteration, retrieval, consultation, disclosure, dissemination or otherwise making available, analysis, erasure or destruction of Personal Data.

Purpose of the transfer and further processing

Processing shall be carried out by Company on order to provide the Services to Customer, as set out in the Main Agreement.

Retention period

Personal Data will be retained for the term of the Main Agreement, or otherwise subject to the retention polices of the parties, commensurate with the requirements of Data Protection Laws.
Annex II – Technical and Organizational Measures including Technical and Organizational Measures to Ensure the Security of the Data

At a minimum, the following technical and organizational measures will be implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, considering the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. Data importer shall take commercially reasonable measures designed to ensure that subprocesses have in place measures that are substantively as or more protective, considering the personal data to be processed by such sub processor.

EX.CO shall at a minimum ensure the following security measures:

- **Information security policy**: EX.CO will implement and adhere to a written information security policy that specifies the security standards it will apply to protect the Personal Data it processes in accordance with this DPA. The information security policy will mandate the use of appropriate technical and organizational security measures in the EX.CO's organization to protect Personal Data against unauthorized and unlawful processing and against accidental loss, damage or destruction. It will further describe the measures to be taken in the event of an actual or suspected data or security breach.

- **Information security officer**: EX.CO will appoint a duly skilled employee with responsibility for ensuring the security of Personal Data processed by EX.CO in its organization and for reviewing, maintaining and updating the Provider’s information security policy.

- **Physical security**: Access to data processing facilities will be restricted to duly authorized employees and contractors by use of keys, fingerprint readers, or other electronic security measures.

- **Firewall and anti-virus**: Where technically feasible, EX.CO will implement an appropriate firewall, anti-virus, anti-spyware and other anti-malware software and technologies on all networks and systems it uses to process Personal Data. EX.CO will update its firewall, anti-virus, anti-spyware and other anti-malware software and technologies on a regular basis to ensure that they protect against then-current virus, spyware and other malware threats.

- **Access controls**: EX.CO will implement technical access controls that restrict access to Personal Data it processes to duly authorized employees and contractors only. Duly authorized employees and contractors will be permitted to access Personal Data only to the extent necessary for the performance of their duties.

- **Usernames / passwords**: Access to Personal Data will be controlled through access privileges (described above), usernames and confidential passwords. No two employees or contractors may share or use the same username. Employees and contractors will be required to create complex passwords consistent with then-current security best practices.

- **Back-up**: EX.CO will take regular, at least weekly, back-ups of the Personal Data that it processes on behalf of Exporter. Data back-ups will be stored securely at an offsite location and will be available for data restoration within a reasonable period of time.

- **Disaster recovery / business continuity**: EX.CO will implement and adhere to appropriate disaster recovery and business continuity plans that will ensure the availability, security, integrity and (where necessary) restoration of the Personal Data on the occurrence of a force majeure or similar
business interruption event. EX.CO will provide a copy of its disaster recovery and business continuity plans upon request.

- **Power loss**: EX.CO’s data processing systems will protect against the loss, destruction, or damage of Personal Data due to failure or interference of any power supply.

- **Audit**: EX.CO will audit its compliance with its information security policy on a regular basis and at least once per annum. Any remedial measures identified as necessary following an audit will be reviewed and implemented as appropriate under the circumstances.