DATA PROCESSING ADDENDUM

Last revised: May 2026

EX.CO Technologies Ltd. or its affiliates ("**Company**") and you ("**Customer**"; each a "**Party**", together the "**Parties**") have entered into a principal agreement ("**Agreement**") in the context of which Personal Data (as defined below) is disclosed to or processed by the Company, and are agreeing to this Data Processing Addendum, including Schedule A and Annexes I-III ("**DPA**"). This DPA is entered into by Company and Customer and supplements the Agreement. This DPA will be effective and replaces any previously applicable terms relating to its subject matter, from the effective date of the Agreement.

If you are accepting this DPA on behalf of Customer, you warrant that: (i) you have full legal authority to bind Customer to this DPA; (ii) you have read and understand this DPA, and (iii) 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 reflects 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:

2.1.1 "**Approved Jurisdiction**" means a jurisdiction approved as having adequate legal protections for data by the European Commission (currently available here), the UK Information Commissioner's Office (currently available here), or the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**") (currently available here), as applicable.

2.1.2 "**Data Protection Law(s)**" means any and all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or federal or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Privacy and Electronic Communications Directive 2002/58/EC (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**"), 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 Israeli Protection of Privacy Law, 5741-1981 and the regulations enacted thereunder, the Swiss Federal Act on Data Protection ("**FADP**"), US Data Protection Laws, and any amendments or replacements to the foregoing.

2.1.3 "**Data Subject**" means a natural person to whom Personal Data relates. Where applicable, the term Data Subject shall include "Consumer", as this term is defined under US Data Protection Laws (as applicable).

2.1.4 "**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 (as defined in the GDPR) or any equivalent term under Data Protection Laws will comprise a Security Incident.

2.1.5 "**Special Categories of Data**" means personal data as defined under Article 9 of the GDPR and where applicable, "Sensitive Personal Information" or other equivalent terms as defined under Data Protection Laws.

2.1.6 "**Standard Contractual Clauses**" means the applicable module 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.

2.1.7 "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, which was entered into force on 21 March, 2022, as available here.

2.1.8 "**US Data Protection Laws**" means any and all applicable acts, directives, decrees, laws, rules, and regulations, and binding regulatory guidance, on any state or federal level, pertaining to data privacy, data security and the protection of Personal Data, including, without limitation, in California, Colorado, Connecticut, Utah, Virginia, Texas, Oregon, Florida, Montana, Iowa, Delaware, New Jersey, New Hampshire, Nebraska, Tennessee, Minnesota, Maryland, Indiana, and Kentucky, as well as any future laws, amendments, or regulations that may be enacted or promulgated governing data protection within the United States.

2.1.9 The terms "**controller**", "**Personal Data**", "**process**(**ing**)", and "**processor**" as used in this DPA have the meanings given to them in Data Protection Laws. Where applicable, controller shall be deemed "**Business**", processor shall be deemed "**Service Provider**" or "**Contractor**", and Personal Data shall be deemed "**Personal Information**" as these terms are defined under US Data Protection Laws.

2.2 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 its provision of the services in connection with the Agreement (the **"Services**");

3.1.2 Data Protection Laws apply to the processing of Personal Data.

4. **Parties' Roles**

4.1 In respect of the Parties' rights and obligations under this DPA regarding the Personal Data, the Parties hereby acknowledge and agree that the Customer is the Controller or Processor (as well as, as applicable, the Business or Service Provider, as these terms are defined under US Data Protection Laws) and Company is a Processor or Sub-Processor (as well as, as applicable, the Service Provider, as this term is defined under the US Data Protection Laws), and accordingly:

4.1.1 Company agrees that it shall process all Personal Data in accordance with its obligations pursuant to this DPA;

4.1.2 The Parties acknowledge that the Customer discloses Personal Data to Company only for the performance of the Services and that this constitutes a valid business purpose for the processing of such data.

4.2 If Customer is a Processor, Customer warrants to Company that Customer's instructions and actions with respect to the Personal Data, including its appointment of Company as another Processor and concluding the Standard Contractual Clauses and/or the UK Addendum (as applicable), have been authorized by the relevant Controller.

4.3 Notwithstanding anything to the contrary in the DPA, Customer acknowledges that Company shall have the right to process Personal Data:

4.3.1 collected in the context of providing the Services to Customer for Company's legitimate internal business purposes, including but not limited to for the purposes of billing, record-keeping, account management, analytics, market research, product improvement and development, support, protection against fraudulent or illegal activity and misuse of the Services, for the purpose of compliance with legal obligations, and the establishment, exercise and defense of legal claims.

4.3.2 The Company may use aggregated and/or anonymized information for any purpose, subject to any applicable confidentiality obligations between the Parties.

4.4 To the extent any data referred to under Section 4.3 above is considered Personal Data, then the Company shall be deemed to be an independent Controller of such data under Data Protection Laws, and its processing shall be outside the scope of this DPA.

5. **Compliance with Laws**

5.1 Each Party shall comply with its respective obligations under Data Protection Laws.

5.2 Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Controller under Data Protection Laws.

5.3 Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this DPA and take reasonable and appropriate measures to remedy such non-compliance.

5.4 Throughout the duration of the DPA, Customer represents and warrants that:

5.4.1 Personal Data has been and will continue to be collected, processed and transferred by Customer to Company in accordance with the relevant provisions of Data Protection Laws;

5.4.2 Customer is solely responsible for determining the lawfulness of the data processing instructions it provides to Company and shall provide Company only with instructions that are lawful under Data Protection Laws;

5.4.3 the processing of Personal Data by Company, as well as any instructions to Company in connection with the processing of the Personal Data ("**Processing Instructions**"), has been and will continue to be carried out in accordance with the relevant provisions of Data Protection Laws; and that

5.4.4 The Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the DPA and obtained any relevant consents or established other lawful grounds thereto (including without limitation any consent required in order to comply with the Processing Instructions).

6. Processing Purpose and Instructions

6.1 The subject matter of the processing, the nature and purpose of the processing, the type of Personal Data and categories of Data Subjects, are described in Annex I attached hereto.

6.2 Company shall process Personal Data only in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Agreement and Data Protection Laws, unless Company is otherwise required to do so by law to which it is subject (and in such a case, Company shall inform Customer of that legal requirement before processing, unless legally prohibited from doing so). Company shall promptly inform Customer if, in Company's opinion, a Processing Instruction is in violation of Data Protection Laws.

6.3 To the extent that the Processing Instructions may result in the processing of any Personal Data outside the scope of the Agreement, then such processing will require prior written agreement between Company and Customer, which may include any additional fees that may be payable by Customer to Company for carrying out such Processing Instructions.

6.4 Company shall not process Personal Data for any purpose other than for the purpose of performing the Services or for a lawful commercial or business purpose (as defined under US Data Protection Laws), or as otherwise permitted under Data Protection Laws. Company's performance of the Services may include disclosing Personal Data to Third Parties and Sub-Processors where such disclosure is necessary for the provision of the Services and Company's activities.

7. Reasonable Security and Safeguards

7.1 Company agrees to use security measures: (i) to protect the availability, confidentiality, and integrity of any Personal Data processed by Company in

connection with this DPA, and (ii) to protect such Personal Data from Security Incidents. Such security measures include the security measures set out in Annex II.

7.2 The security measures are subject to technical progress and development, and Company may update or modify the security measures from time to time provided that such updates and modifications shall not, in the Company's discretion, result in the degradation of the overall security of the Services.

7.3 Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who has access to and processes Personal Data. Company shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8. **Security Incidents**

Upon becoming aware of a Security Incident, Company will notify Customer without undue delay and will provide information relating to the Security Incident as required under Data Protection Laws. Company will make reasonable endeavors, at Customer's expense, to assist Customer in mitigating, where possible, the adverse effects of any Security Incident.

9. **Security Assessments and Audits**

9.1 Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company, and may result in generation of an audit report ("**Report**"), which will be Company's confidential information.

9.2 Company shall, upon prior written notice and subject to obligations of confidentiality, no more than once a year and in normal business hours, allow its data processing procedures and documentation to be inspected by Customer (or a designee mutually agreed upon by the Parties), at Customer's expense, in order to ascertain compliance with this DPA; Company shall cooperate in good faith with such audit requests by providing access to relevant knowledgeable personnel and documentation.

9.3 At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with a copy of the Report, if available, so that Customer can reasonably verify Company's compliance with its obligations under this DPA.

10. **Cooperation and Assistance**

10.1 If Company receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data as part of the provision of its Services to Customer, including requests from individuals seeking to exercise their rights under applicable Data Protection Law, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If

Company is required to respond to such a request, Company will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so. The Customer is responsible for verifying that the requestor is the Data Subject whose information is being sought or its duly authorized representative. Company bears no responsibility for information provided in good faith to Customer in reliance on this subsection.

10.2 If Company receives a legally binding request for the disclosure of Personal Data which is subject to this DPA, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. It is hereby clarified however that if no response is received from Customer within three (3) business days (or such shorter period as required by applicable law or the relevant authority), Company shall be entitled to provide such information.

10.3 Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data. Customer shall cover all costs incurred by the Company in connection with its provision of such assistance.

10.4 Upon reasonable notice, Company shall:

10.4.1 taking into account the nature of the processing, provide reasonable assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligation to respond to requests for exercising Data Subjects' rights, at Customer's expense;

10.4.2 provide reasonable assistance to the Customer in ensuring Customer's compliance with its obligation to carry out data protection impact assessments or prior consultations with data protection authorities with respect to the processing of Personal Data, provided, however, that if such assistance entails any costs or expenses to Company, the Parties shall first come to an agreement on Customer reimbursing Company for such costs and expenses.

11. **Use of Sub-Processors**

11.1 Customer provides a general authorization to Company to subcontract (and permit each Sub-Processor appointed in accordance with this Section to subcontract) its obligations under this DPA to another person or entity ("**Sub-Processor(s)**") in accordance with this Section.

11.2 Company may continue to use those Sub-Processors already engaged by Company as at the date of this DPA, as specified in Annex III, subject to Company, in each case as soon as practicable, meeting the obligations set out in this Section.

11.3 Company can at any time appoint a new Sub-Processor provided that Customer is given ten (10) days' prior notice and the Customer does not legitimately object to such changes within that time frame. Legitimate objections must contain reasonable and documented grounds relating to a Sub-Processor's non-compliance with Data Protection Laws. If, in Company's reasonable opinion, such objections are legitimate, Company shall either refrain from using such Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Sub-Processor. Where Company

notifies Customer of its intention to continue to use the Sub-Processor in these circumstances, Customer may, by providing written notice to Company, terminate the affected portion of the Services.

11.4 With respect to each Sub-Processor, Company shall ensure that the arrangement between Company and the Sub-Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this DPA and meets the requirements of Data Protection Laws.

11.5 Company will be responsible for any acts or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this DPA.

12. **Transfer of EEA Residents' Personal Data Outside the EEA**

12.1 To the extent that Company processes Personal Data outside the EEA, UK, Switzerland, or an Approved Jurisdiction, then the Parties shall be deemed to enter into the Standard Contractual Clauses and UK Addendum (as applicable), subject to any amendments contained in Schedule A, in which event the Customer shall be deemed as the Data Exporter and the Company shall be deemed as the Data Importer (as these terms are defined therein).

12.2 Company may transfer Personal Data of residents of the EEA, Switzerland, or the UK outside the EEA, Switzerland, the UK, or an Approved Jurisdiction, provided that such transfer is: (i) subject to appropriate safeguards (for example, through the use of the Standard Contractual Clauses, or other applicable frameworks), or (ii) in accordance with any of the exceptions listed in the Data Protection Laws (in which event Customer will inform Company which exception applies to each transfer and will assume complete and sole liability to ensure that the exception applies).

13. **Data Retention and Destruction**

Company will only retain Personal Data for the duration of the Services or as required to perform its obligations under the Agreement, or as otherwise required to do so under applicable laws or regulations. Following expiration or termination of the Services, Company will delete or return to Customer all Personal Data in its possession, except to the extent Company is required under applicable laws to retain the Personal Data. The terms of this DPA will continue to apply to such Personal Data. This section shall not apply to the activities that are the subject matter of section 4.3 herein.

14. **Obligations under US Data Protection Laws**

14.1 To the extent that Company processes Personal Data which is subject to the US Data Protection Laws, then in addition to the obligations set out herein, Company shall not:

14.1.1 process the Personal Data other than on Customer’s documented instructions;

14.1.2 Sell or Share Personal Data (as the terms "Sell" and "Share" are defined under US Data Protection Laws) disclosed to or collected by it (or on its behalf) in connection with the Services;

14.1.3 retain, collect, use or disclose Personal Data disclosed to it or collected by it (or on its behalf), for any purpose other than for the business purpose, unless otherwise permitted under US Data Protection Laws;

14.1.4 combine the Personal Data of Data Subjects that it collects, receives from, or on behalf of, the Customer with Personal Data that the Company receives from, or on behalf of, another person or persons or collects from its own interaction with Data Subjects unless and solely to the extent necessary to perform the business purpose, unless otherwise permitted under US Data Protection Laws.

14.2 Company acknowledges and understands its obligations under this Section and will comply with them.

15. **General**

15.1 Any claims brought under this DPA will be subject to the Agreement, including any exclusions and limitations set forth therein.

15.2 In the event of a conflict between the Agreement (or any document referred to therein) and this DPA, the provisions of this DPA shall prevail.

15.3 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; (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. Company will use commercially reasonable efforts to inform Customer at least thirty (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.

Schedule A – Standard Contractual Clauses and the UK Addendum

1. If Customer is a Controller – the Parties shall be deemed to enter into the Controller to Processor Standard Contractual Clauses (Module Two); if Customer is a Processor – the Parties shall be deemed to enter into the Processor to Processor Standard Contractual Clauses (Module Three).

2. This Schedule A sets out the Parties' agreed interpretation of their respective obligations under Module Two or Module Three of the Standard Contractual Clauses (as applicable).

3. The Parties shall complete Annexes I–III below, which are incorporated in the Standard Contractual Clauses by reference.

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

    4.1 Clause 7 of the Standard Contractual Clauses shall not be applicable.
    4.2 In Clause 9, option 2 shall apply. Company shall inform the Customer in writing of any intended changes ten (10) days in advance.
    4.3 In Clause 11, data subjects shall not be able to lodge a complaint with an independent dispute resolution body.
    4.4 In Clause 13, the applicable supervisory authority shall be the Irish Data Protection Commissioner.
    4.5 In Clause 17, option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Ireland.
    4.6 In Clause 18(b) the Parties choose the courts of Dublin.

5. To the extent the UK Addendum applies, the following shall apply:

    5.1 All the information provided under the Standard Contractual Clauses shall apply to the UK Addendum with the necessary changes per the requirements of the UK Addendum. Annexes 1A and 1B shall be replaced with Annex I below; Annex II shall be replaced with Annex II below, and Annex III shall be replaced with Annex III below.
    5.2 In Table 4 of the UK Addendum, either party may terminate the agreement in accordance with section 19 of the UK Addendum.
    5.3 By entering into this DPA, the Parties hereby agree to the changes made to the UK Addendum.

6. To the extent the FADP applies, the following shall apply:

6.1 references to the GDPR are to be understood as references to the FADP;
6.2 the competent supervisory authority shall be the FDPIC;
6.3 references to 'EU', 'Union' and 'Member State' are replaced with 'Switzerland';
6.4 In Clause 17, Option 1 shall apply. The Parties agree that the clauses shall be governed by the law of Switzerland;
6.5 In Clause 18(b) the Parties choose the courts of Zurich, Switzerland as their choice of forum and jurisdiction.

Annex I – Description of Processing Activities

A. **Identification of Parties**

"**Data Exporter**": the Customer;

"**Data Importer**": the Company.

B. **Description of Transfer**

Categories of data subject:	Customer's end-users
Categories of Personal Data	• Device identifiers and internet or electronic network activity (e.g., IP addresses, GAID/IDFA, browsing history, timestamps, etc.) • Geo-location information (non-precise)
Special Categories of Data/Sensitive Personal Information	None
Nature of Processing	• Analytics • Advertising (including auditing related to Advertising) • Security, integrity and maintaining quality of the Company's services • Transient use
Frequency of Transfer	Continuous
Purpose of the transfer and further processing	As set forth in the Agreement
Retention period	Personal Data will be retained for the term of the Agreement.

Annex II – Technical and Organizational Measures to Ensure the Security of the Data

This Annex forms part of the DPA and describes the technical and organizational security measures implemented by the data importer.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Annex III – List of Sub-processors

Below is the list of the Data Importer's Sub-processors:

#	Name	Location	Description of Processing
1.	AWS Athena	United States	Database management.
2.	CheckPoint	USA	Cloud email security, anti-phishing, DLP for email.
3.	Datadog	United States	Infrastructure monitoring.
4.	Fastly	worldwide	Content delivery, edge compute, DDoS, WAF.
5.	Google Ad Manager	worldwide	Ad serving, programmatic monetization, reporting.
6.	Google BigQuery	United States	Database management.
7.	Groundcover	USA	eBPF observability.
8.	HUMAN Security	United States	Bot detection, ad fraud prevention, web traffic analysis.
9.	Integral Ad Science	United States	Ad verification, viewability, brand safety, fraud detection.
10.	IntentIQ	USA	Identity resolution.
11.	Looker Studio	USA	Dashboard reporting, data visualization .
12.	Middle Block	USA	Programmatic advertising services.
13.	MongoDB	United States	Database management.
14.	Monte Carlo Data	United States	Data quality monitoring, lineage, anomaly detection.
15.	Redis	United States	Database management.
16.	Salesforce	United States	Customer relationship management.
17.	Zendesk	United States	Customer support.