Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms an integral part of the Devtodev Terms of Use, available at https://www.devtodev.com/terms-of-use/, or similar agreement (including any exhibits, appendices, annexes, terms, orders or policies referenced therein) ("**Agreement**"), entered into by and between **Customer** and **Devtodev** that governs Customer's use and Devtodev's provision of Devtodev's Services.

Customer and Devtodev are hereinafter jointly referred to as the "**Parties**" and individually as the "**Party**". Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

Instructions

This Data Protection Addendum has been pre-signed on behalf of Devtodev. To complete this Addendum, please fill in your details and sign in the relevant signature blocks and send the completed and signed DPA to Devtodev by email to info@devtodev.com.

In all cases where a specific term in an Agreement incorporates the DPA into the Agreement by reference, the DPA shall be deemed executed upon execution of the Agreement and will be legally binding and made an integral part of the Agreement.

1. Definitions. In addition to capitalized terms defined elsewhere in this DPA or the Agreement, the following terms shall have the meanings ascribed to them herein.

1.1. "**Affiliate**" means any entity that directly or indirectly controls is controlled by, or is under common control with the subject entity. "**Control**" for purposes of this definition means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.2. "**CCPA**" means the California Consumer Privacy Act and its amendments, including the California Privacy Rights Act ("**CPRA**").

1.3. "**Controller**" means the natural person or entity that determines the purposes and means of the processing of Personal Data or otherwise is in charge of making decisions regarding the processing of Personal Data, including a "Business" as defined under the CCPA.

1.4. "**Data Protection Authorities**" means any competent governmental privacy and data protection authority having jurisdiction over the Processing performed under the Agreement; including a "Supervisory Authority" as defined under the GDPR.

1.5. "**Data Protection Laws**" means the applicable data protection or privacy laws in the European Union ("**EU**"), European Economic Area ("**EEA**") and their Member States, the United Kingdom ("UK") and the United States including the GDPR, UK GDPR, and CCPA as well as other similar applicable worldwide data protection laws that relate to the protection of Personal Data.

1.6. "**Data Subject**" means the identified or identifiable person to whom Personal Data relates.

1.7. "**GDPR**" means EU General Data Protection Regulation 2016/679.

1.8. “**Member States**” means a member of the EU.

1.9. “**Personal Data**” means any information that relates to an identified or identifiable natural person and is protected under Data Protection Laws and Processed by Devtodev in the provision of its Services pursuant to the Agreement.

1.10. “**Processing**” means any operation or set of operations performed upon Personal Data or 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.

1.11. “**Processor**” means a natural person or entity that processes personal data on behalf of the Controller, including a “Service Provider” as defined under the CCPA.

1.12 “**Standard Contractual Clauses**” means the contractual clauses established by the European Commission concerning the international transfer of Personal Data, as set out in Schedule 2.

1.13. “**Sub Processor**” means any Processor appointed by or on behalf of Devtodev or any Devtodev Affiliate to Process Personal Data on behalf of the Customer in connection with the Agreement.

1.14. “**UK GDPR**” means the UK’s General Data Protection Regulation and other applicable data protection laws of the UK.

2. **Processing of Customer Personal Data.**

2.1. The Parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, and Devtodev is the Processor. Devtodev shall not Process Customer Personal Data other than on the Customer’s documented reasonable and customary instructions, as specified in the Agreement or this DPA, unless such Processing is required by applicable laws to which Devtodev is subject.

2.2. Customer instructs Devtodev to Process Customer Personal Data in a manner consistent with the terms of the Agreement and this DPA.

2.3. Customer warrants and represents that its instructions to Process Personal Data comply with Data Protection Laws. Customer shall be solely responsible for the accuracy and legality of the Personal Data and for ensuring it has an appropriate lawful basis and right to enable the Processing of Personal Data pursuant to the terms of the Agreement and this DPA. Customer specifically acknowledges and agrees that its use of the Services will not violate the rights of any Data Subject.

2.4. Schedule 1 sets forth the details of the Processing of Customer Personal Data. In no event shall Customer configure the Services to collect or cause Devtodev to Process Personal Data that is beyond the scope set forth in Schedule 1, including, specifically, any Restricted Data (as defined in the Agreement or, if undefined, then shall mean any Personal Data beyond the scope of the of Personal Data specified in Schedule 1).

3. **California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA).**

3.1. To the extent any Customer Data is deemed “Personal Information” (as such term is defined under the CCPA) and is subject to the CCPA, Devtodev agrees not to:

(a) "sell" or "share" the Personal Information as such terms are defined under the CCPA;

(b) retain, use, or disclose Personal Information for any purpose other than for the specific purpose of performing the Services or as otherwise expressly permitted under the Agreement, including retaining, using, or disclosing the Personal Data for a commercial purpose other than the business purposes specified in this DPA or the Agreement, or as otherwise permitted by the CCPA;

(c) retain, use, or disclose the Personal Information outside of the direct business relationship with Customer;

(d) combine Personal Information it receives from Customer with Personal Information it receives from or on behalf of another person or collects from its own interactions with consumers, except where required to provide the Service, provided it is permitted under the CCPA.

4. **Devtodev Personnel.** Devtodev shall take reasonable steps to ensure that access to the Customer Personal Data is limited on a need to know/access basis and that all Devtodev personnel receiving such access are subject to confidentiality undertakings or professional or statutory obligations of confidentiality in connection with their access/use of Customer's Personal Data.

5. **Security.** Devtodev shall, in relation to the Customer Personal Data, implement appropriate technical and organizational measures to ensure an appropriate level of security, including, as appropriate and applicable, the measures referred to in Article 32(1) of the GDPR, as set out in Schedule 4 herein. In assessing the appropriate level of security, Devtodev shall take into account the risks that are presented by Processing Personal Data, in particular risks arising from a Personal Data Breach.

6. **Sub-Processing**.

6.1. Customer authorizes Devtodev and each Devtodev Affiliate to appoint (and permit each Sub Processor appointed in accordance with this Section 6 to appoint) Sub Processors in accordance with this Section 6 and any restrictions in the Agreement.

6.2. The Sub Processors used by Devtodev are specified at: https://www.devtodev.com/subprocessors ("**Sub Processors Website**").

6.3. Devtodev may appoint new Sub Processors at any time and shall update the Sub Processors Website upon such appointments. If the Customer wishes to receive notice of any new Sub Processors, it may request to receive such notice by following the updates on the Sub Processors Website. If, within ten (10) days of such notice, Customer notifies Devtodev in writing of any reasonable objections to the proposed appointment, Devtodev shall not utilize such Sub Processor to Process Customer Personal Data until reasonable steps have been taken to address the objections raised by Customer, such as a change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub Processor. Where such steps are not sufficient to relieve Customer's reasonable objections and a solution has not been found within a reasonable period of time, which shall not exceed twenty (20) days from Customer's objection notification, then Customer or Devtodev may, by written notice to the other Party, with immediate effect, terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub Processor, without bearing liability for such termination.

6.4. With respect to each Sub Processor, Devtodev shall: (a) take reasonable steps to ensure that the Sub Processor is committed to providing the level of protection for Personal Data required by the Agreement; (b) ensure that the arrangement between Devtodev and the Sub Processor is governed by a written contract, including terms which, to the extent applicable to the nature of services provided by the Sub Processor, offer a level of protection that, in all material respects, are consistent with the levels set out in this DPA and the Agreement; and (c) remain fully liable to the Customer for the performance of the Sub Processor's data protection obligations where the Sub Processor fails to fulfill such obligations.

7. **Data Subject Rights**.

7.1. Customer shall be solely responsible for compliance with any statutory obligations concerning requests to exercise Data Subject rights under Data Protection Laws (e.g. for access, rectification or deletion of Customer Personal Data, etc.). To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject request, taking into account the nature of the Processing, Devtodev shall reasonably assist Customer, insofar as feasible, to fulfill Customer's said obligations with respect to such Data Subject requests, as applicable, at Customer's sole expense. Customer acknowledges and agrees that any requests for bulk deletion of Customer Personal Data may require significant effort (at least 90 days) and costs and thus may be subject to additional fees. Customer shall therefore notify Devtodev at the earliest possible instance that Customer requires such bulk deletion, upon which the Parties shall coordinate in good faith any associated fees and timelines.

7.2. Devtodev: (a) shall promptly notify Customer if it receives a request from a Data Subject under any Data Protection Law in respect of Customer Personal Data (unless prohibited by applicable law); and (b) shall not respond to that request except on the documented instructions of Customer or as required by applicable laws. Notwithstanding the foregoing, Devtodev shall be permitted to respond (including through automated responses) to any such requests, informing the Data Subject that his request has been received and/or with instructions to contact Customer in the event that his request relates to Customer.

8. **Personal Data Breach**.

8.1. Devtodev shall notify Customer, without undue delay, upon Devtodev becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed by Devtodev ("**Personal Data Breach**"). In such event, Devtodev shall provide Customer with any relevant information (to the extent in Devtodev's reasonable possession and/or control) to assist Customer in meeting any obligations to inform Data Subjects or Data Protection Authorities of the Personal Data Breach under the Data Protection Laws.

8.2. Devtodev shall take the necessary steps for the mitigation and remediation of each such Personal Data Breach at its sole discretion and expense (except to the extent caused by Customer) and shall provide Customer with a summary of the material steps taken. To the extent Customer requests Devtodev to conduct any additional measures, then any such measures which Devtodev agrees to implement (at its sole discretion), shall be executed at Customer's sole expense.

9. **Data Protection Impact Assessment and Prior Consultation**.

9.1. At the written request of the Customer, Devtodev and each Devtodev Affiliate shall provide reasonable assistance to Customer, at Customer's expense, with any data protection impact assessments or prior consultations with Data Protection Authorities, as required under any applicable Data Protection Laws. Such assistance shall be solely in relation to the Processing of Customer Personal Data by Devtodev.

10. **Deletion or return of Customer Personal Data**.

10.1. Following termination of the Agreement, Personal Data shall be deleted or otherwise made unrecoverable and/or anonymized, other than such copies, as authorized under the Agreement or this DPA, or required, to be retained in accordance with applicable law and/or regulation.

11. **Audit Rights**.

11.1. Subject to sections 11.2 and 11.3, Devtodev shall make available to Customer on request such information necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits by a reputable auditor mandated by Customer in relation to the Processing of Customer Personal Data by Devtodev.

11.2. To the extent Devtodev has undergone a third-party independent audit based on SOC 2, Type II or similar standards, then any audit right arising pursuant to section 11.1 shall be first satisfied by providing Customer with a summary of the report of such audit. If Customer, for reasonable reasons, is not satisfied by the summary of the independent audit report then Customer may request that a reputable auditor perform an audit pursuant to section 11.1 and subject to Section 11.3. If Devtodev does not agree to such additional audit or inspection, then Customer shall have the right to terminate the Agreement with immediate effect.

11.3. Customer shall give Devtodev reasonable prior written notice of any audit or inspection to be conducted under Section 11.1 and shall use (and ensure that each of its mandated auditors uses) its best efforts to avoid causing any damage, injury, or disruption to Devtodev's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. All such audits shall be subject to the confidentiality obligations set forth in the Agreement. Customer and Devtodev shall mutually agree upon the scope, timing, and duration of the audit or inspection in addition to any reimbursement of expenses for which Customer shall be responsible. Any such audits shall not occur more than once a year (except where required by law or due to a Personal Data Breach). Additionally, Devtodev need not give access to its premises for the purposes of such an audit or inspection: (a) to any individual unless he or she produces reasonable evidence of identity and authority; (b) to any competitor of Devtodev; or (c) outside Devtodev's normal business hours. The Customer shall share the full audit report with Devtodev and shall not share it with any third party except its accountants and legal advisors, who are bound to confidentiality. The Customer shall not use such audit report for any other purpose than to assess Devtodev's compliance with this DPA.

12. **Transfers**

12.1. Customer acknowledges that Devtodev may transfer and Process Personal Data outside of the country from which it originated in order to perform the services for Customer, including to such countries identified on the Sub Processors Website. The Customer shall ensure it obtains any necessary consents or has the necessary rights to enable such transfer. Subject to the foregoing, Devtodev shall only make such transfers in compliance with Data Protection Laws. With respect to any transfers of Personal Data under the Agreement from the EU, EEA, Member States, and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws or which transfer is not otherwise governed by a framework approved by the European Commission to which Devtodev is officially certified, such transfers shall be subject to the Standard Contractual Clauses ("**SCCs**") attached hereto as Schedule 2. The Standard Contractual Clauses shall come into effect and be deemed executed upon execution of this DPA and shall apply pursuant to the order of precedence described in the preceding sentence.

12.2. If the Processing of Personal Data involves the transfer of Personal Data of Data Subjects in the UK to any country that has not received an adequacy decision, the Parties hereby incorporate and agree to comply with the SCCs and the UK International Data Transfer Addendum to the EU Commission SCCs attached hereto as Schedule 3.

13. **General Terms**.

13.1. **Agreement and Order of Precedence**. Nothing in this DPA reduces either Party's obligations under the Agreement in relation to the collection, use, processing, and protection of Personal Data. Any claims brought under this DPA shall be subject to the terms of the Agreement, including, without limitation, choice of jurisdiction, governing law, and any liability limitations or exclusions. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing and signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail. In the event of any conflict or inconsistency between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.2. **Severance**. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall either be: (i) amended as necessary to ensure its validity and enforceability while preserving the Parties' intentions as closely as possible, or, if this is not possible; (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, this DPA is entered into and becomes a binding part of the Agreement with effect from the later date set out below.

Customer.

Company Name: ____________

Signature: ________________

Name: ___________________

Title: ____________________

Date: ____________________

Devtodev Ltd.

Signature:

Name:

Title: CEO

Date:

SCHEDULE 1: DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This **Schedule 1** includes certain details of the Processing of Customer Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Customer Personal Data. The subject matter of the Processing of the Customer Personal Data is to provide measurement and analytics services, as are further described in the Agreement. The duration shall be for the period of the Agreement.

The nature and purpose of the Processing of Customer Personal Data: rendering Services in the nature of an analytics platform, as further detailed in the Agreement.

The types of Customer Personal Data to be Processed are as follows:
The data types that may be processed when using the services:

a. "Device Information": this refers to technical information related to an End User's mobile device or computer, such as device type and model, system language, OS type and version, rooted/jailbroken OS Flag, screen settings (resolution, PPI), app version, push token time stamp and zone.

b. "Identifiers": this refers to various identifiers that generally only identify a computer, device, browser or Application. For example, IP address (which may also provide general location information), User agent strings, Mobile Device Advertising Identifiers such as IDFA (identifier for advertisers) and Android ID (in Android devices); IDFV (ID for Vendors in iOS), Google Advertiser ID, Serial ID, Customer issued user ID and other similar identifiers including those generated by Devtodev to enable provision of the Services.

c. "Engagement Information": this refers to information relating to End User actions within an app such as session start, activity period, source of install, install date, last use date, links clicked, pages visited, in-app purchases made, and other payment-related player data (such as transaction ID, time and amount), progress within a game, cheater status flags, use of app functions and features including use of social networking links and other interactions, events and action Customers choose to measure and analyze within their Application (including advertising campaign related data – eg. advertising clicked or viewed, attribution data). For the specific privacy practices and data collected by an app using our Services please visit the app's own privacy policy.

- Any other data types explicitly agreed by the Parties under the Agreement.

For clarity, Customer shall not configure the Services to collect any data that is not permitted to be collected pursuant to the terms of the Agreement or that is beyond the scope identified above.

The categories of Data Subject to whom the Customer Personal Data relates are as follows:
End users who use or interact with Customer's websites, products, services, advertisements and mobile application services.

SCHEDULE 2 – EU SCCs

The Terms of the EU Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "**EU SCCs**") shall be incorporated by reference to the DPA as follows:

1. The Module applicable to the transfer of Controller Personal Data originating from the EU under the Agreement is Module 2 – "Controller to Processor."

2. The following selections are made where Commission Implementing Decision (EU) 2021/914 permits the selection of options in the Clauses of the EU SCCs:

    a. Clause 7 "Optional (Docking Clause)" – retained.

    b. Clause 9 "Use of Subprocessors" sub-section (a) – Option 2 (general authorization) is selected.

    c. Clause 11 "Redress" – sub-section (a) – the option provided in this sub-section is not selected.

    d. Clause 17 "Governing Law" – Option 1 is selected, and the governing law is as follows:

    "These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland."

    e. Clause 18 "Choice of Forum and Jurisdiction" sub-section (b) is amended as follows: "The Parties agree that those shall be the courts of Dublin, Ireland."

3. Annex IA to the SCCs shall be considered filled as follows: the Data Exporter is the Customer, and the Exporter's details are the same as the Customer's details as set out in the Order Form.
4. Annex IB to the SCCs shall be the same as Schedule I to the DPA and in addition the following details are included to complete Annex IB: the frequency of the transfer is continuous.
5. Annex IC is completed as follows: The Supervisory Authority of the Republic of Ireland.
6. Annex II to the SCCs shall be the same as Schedule 4 to the DPA.
7. Annex III to the SCCs shall be the same as Schedule 5 to the DPA.

***

SCHEDULE 3 – UK SCCs

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties’ details	Full legal name: Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Devtodev Ltd. Main address (if a company registered address): Sapir St. 1, Herzliya, Israel, 4685205 Official registration number (if any) (company number or similar identifier): 516835758
Key Contact	Job Title: Contact details, including email:	Full Name (optional): Job Title: Devtodev Privacy Team Contact details including email: info@devtodev.com
Signature (if required for the purposes of Section 2)	This IDTA is deemed signed upon signing the DPA.	This IDTA is deemed signed upon signing the DPA.

Table 2: Selected SCCs, Modules, and Selected Clauses

Addendum EU SCCs		The version of the Approved EU SCCs, which this Addendum is appended to, is detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses, or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	2	Yes	N/A	Option 2 General	10 days	No

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: shall be the same as the parties set out in Table 1: Parties of this Schedule 3 to the DPA
Annex 1B: Description of Transfer: shall be the same as in Schedule 1 to the DPA.
Annex II: Technical and organizational measures, including technical and organizational measures to ensure the security of the data: shall be the same as Schedule 4 to the DPA.
Annex III: List of Subprocessors: shall be the same as Schedule 5 to the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer Exporter neither Party

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

SCHEDULE 4 - SECURITY MEASURES

At Devtodev, we are committed to protecting the confidentiality, integrity, and availability of customers' data. To achieve this, we have implemented a number of organizational and technical measures, as well as physical and policy-based measures, to secure our platform and safeguard our customer's data as specified below. Devtodev may update the measures from time to time, without notice (except where there is a degradation in the level of security), to meet evolving industry standards, regulations or controls and as deemed necessary by Devtodev to maintain and provide the services to customers in a secure manner.

1. Devtodev maintains appropriate technical and organizational measures. Under its security program, Devtodev continuously monitors for potential risks and implements appropriate controls to maintain the security and confidentiality of customer data and to protect it from known or reasonably anticipated threats or hazards. The security program is regularly reviewed by a dedicated security team to ensure its effectiveness. The Devtodev team regularly reviews security plans for all networks, systems, and services, monitors for suspicious activity on Devtodev's networks, addresses information security threats, performs routine security evaluations and audits and performs regular security assessments.

2. Devtodev employs industry security standards and which include: (i) change management procedures to ensure that there is no adverse impact on security when changes are performed; (ii) regular code reviews, including through automated static code scanning; and (iii) periodic (at least annually) penetration testing.

3. Devtodev maintains a formal process for granting, modifying, and revoking user access rights to its various systems, including production systems. Access controls are based on job function and role using the concepts of least privilege and need-to-know. Access is provided through the use of unique ID's and a complex password policy.

4. Devtodev utilizes encryption technologies for customer data, as appropriate, in transit and rest. Traffic transferred to Devtodev over HTTPS is encrypted using TLS1.3 encryption (or similar). Customer data is encrypted at rest on our databases through AES256 bit (or similar).

5. Devtodev utilizes industry-standard tools (firewalls, antivirus) to protect against various network threats and vulnerabilities.

6. Devtodev's hosting services maintain various physical security measures over their data hosting locations, including: (i) controlled access and 24-hour security; (ii) surveillance measures; (iii) room security measures (e.g biometric access); (iv) multiple power feeds; and (v) fire detection and suppression systems.

7. Devtodev performs regular certification and third-party audits of its security program (ISO 27001.)

SCHEDULE 5 - SUB-PROCESSORS

https://www.devtodev.com/subprocessors/