

INVO NETWORK

DATA PROCESSING ADDENDUM

Effective Date: October 13, 2026

This Data Processing Addendum ("DPA") forms part of the INVO Developer Terms of Service (the "Terms") between Invo Tech, Inc. ("Invo") and the Developer that has accepted the Terms ("Developer"). It applies automatically, without signature, whenever Invo processes Developer Personal Data under the Terms. Where Developer and Invo have a separate signed commercial agreement, this DPA applies to that agreement too. Capitalized terms not defined here have the meanings in the Terms.

1. Definitions

"Applicable Data Protection Law" means all laws on privacy and the processing of personal data that apply to a party's processing under the Terms, including the EU General Data Protection Regulation 2016/679 ("GDPR"), the GDPR as it forms part of UK law ("UK GDPR"), the Swiss Federal Act on Data Protection, the California Consumer Privacy Act as amended ("CCPA"), and other U.S. state privacy laws.

"Developer Personal Data" means personal data that Invo processes on Developer's behalf and on Developer's instructions under the Terms, as described in Schedule 1.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Developer Personal Data.

"Standard Contractual Clauses" or "SCCs" means the clauses adopted by the European Commission in Implementing Decision (EU) 2021/914, and, for the United Kingdom, the International Data Transfer Addendum issued by the UK Information Commissioner.

"Subprocessor" means any third party Invo engages to process Developer Personal Data.

"Controller", "processor", "data subject", "personal data", "processing", "business", "service provider" and "sell" or "share" have the meanings given in Applicable Data Protection Law.

2. Roles and scope

2.1 Developer as controller, Invo as processor. For Developer Personal Data, Developer is the controller and Invo is the processor (under the CCPA, Developer is the business and Invo is the service provider).

2.2 Invo as independent controller. Invo is an independent controller, and this DPA does not apply, for personal data that Invo processes for its own purposes, namely:

- (a) INVO account, identity, consent, verification and cross-Game identity records for Players;
- (b) payment, payout, Payee and Developer account records, including all Payee Data under Section 5.6 and Section 8.10 of the Terms;
- (c) financial and tax records for sales where Invo is the merchant of record;
- (d) fraud prevention, security, sanctions screening and legal compliance processing; and
- (e) data Invo must keep to meet its own legal obligations.

Invo processes that data under its Privacy Policy.

2.3 Scope. This DPA applies only to processing of Developer Personal Data described in Schedule 1.

3. Developer's instructions

3.1 Invo processes Developer Personal Data only on Developer's documented instructions. The Terms, this DPA, Developer's configuration of the Platform and Developer's API calls are Developer's complete instructions. Additional instructions must be agreed in writing.

3.2 Invo will tell Developer if, in Invo's opinion, an instruction infringes Applicable Data Protection Law, and may suspend that processing until the instruction is changed.

3.3 Invo will not sell or share Developer Personal Data, retain, use or disclose it outside the direct business relationship with Developer, or combine it with personal data Invo receives from others, except as Applicable Data Protection Law permits a processor or service provider to do, including to operate the cross-Game features a Player uses, to detect fraud and security incidents, and to comply with law.

3.4 Developer is responsible for the lawfulness of its instructions and for having a lawful basis, and any notices and consents required, for Invo's processing of Developer Personal Data.

4. Confidentiality

Invo ensures that everyone it authorizes to process Developer Personal Data is bound by a duty of confidentiality, whether by contract or by law, and has access only as needed for their role.

5. Security

5.1 Invo implements and maintains appropriate technical and organizational measures to protect Developer Personal Data, taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of the processing. These measures include:

- (a) encryption of Developer Personal Data in transit and of sensitive fields at rest;
- (b) access controls based on role and least privilege, with multi-factor authentication for administrative access;
- (c) logging and monitoring of access to systems that hold Developer Personal Data;
- (d) separation of production and test environments;
- (e) backup and recovery procedures;
- (f) secure software development and change management;
- (g) vendor security review for Subprocessors; and
- (h) incident response procedures.

5.2 Invo may update these measures from time to time, provided that the overall level of protection is not reduced.

6. Subprocessors

6.1 Developer gives Invo general authorization to engage Subprocessors. Invo engages Subprocessors in the following categories: cloud hosting and infrastructure; data storage and backup; payment processing and banking; identity, document and bank account verification; sanctions screening and fraud prevention; email, push and messaging delivery; customer support tools; and monitoring and analytics.

6.2 Invo maintains a current list of its Subprocessors, with their category and location, and makes it available to Developer on request.

6.3 Invo will give Developer at least thirty (30) days' notice through the Developer dashboard before adding or replacing a Subprocessor, except where a change is needed urgently to protect the security or continuity of the Platform, in which case Invo will give notice as soon as practicable.

6.4 Developer may object to a new Subprocessor on reasonable data protection grounds by written notice within the notice period. The parties will discuss the objection in good faith. If Invo cannot reasonably address it, Developer may stop using the affected part of the Platform, or terminate the Terms, as its sole remedy.

6.5 Invo imposes on each Subprocessor, by written contract, data protection obligations no less protective than those in this DPA, and remains responsible to Developer for each Subprocessor's performance of those obligations.

7. International transfers

7.1 Invo is based in the United States and may process Developer Personal Data in the United States and in other countries where Invo or its Subprocessors operate.

7.2 Where Developer Personal Data is transferred from the European Economic Area, the United Kingdom or Switzerland to a country without an adequacy decision, the parties incorporate the SCCs into this DPA by reference, as follows:

- (a) Module Two (controller to processor) applies where Developer is a controller, and Module Three (processor to processor) applies where Developer is itself a processor;
- (b) Clause 7 (docking clause) applies;
- (c) under Clause 9, Option 2 (general written authorization) applies, with the notice period in Section 6.3;
- (d) the optional wording in Clause 11 does not apply;
- (e) under Clause 17, Option 1 applies and the SCCs are governed by the law of Ireland;
- (f) under Clause 18, disputes are resolved before the courts of Ireland;
- (g) Annex I is completed by Schedule 1, and Annex II by Section 5 of this DPA; and

(h) for UK transfers, the UK International Data Transfer Addendum applies, with its tables completed by the information in this DPA, and for Swiss transfers, references to the GDPR are read as references to the Swiss Federal Act on Data Protection and the competent authority is the Swiss Federal Data Protection and Information Commissioner.

7.3 If the SCCs conflict with this DPA, the SCCs control.

8. Data subject requests

8.1 Invo will forward to Developer, without undue delay, any request it receives from a data subject about Developer Personal Data that identifies Developer, and will not respond except to confirm the request was forwarded, unless Developer instructs otherwise or the law requires.

8.2 Taking into account the nature of the processing, Invo will help Developer, through the Platform's features or otherwise, to respond to data subject requests for access, correction, deletion, restriction, portability and objection. Invo provides deletion and export tools for Player data through the Platform.

9. Personal Data Breaches

9.1 Invo will notify Developer without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a Personal Data Breach affecting Developer Personal Data.

9.2 The notice will describe, as far as then known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Invo will provide further information as it becomes available.

9.3 Invo will take reasonable steps to contain and remedy the breach and will cooperate with Developer's reasonable requests to meet Developer's own notification obligations. Notifying Developer is not an admission of fault.

10. Assistance

Taking into account the nature of the processing and the information available to it, Invo will provide reasonable assistance to Developer with data protection impact assessments and prior consultations with supervisory authorities that relate to Invo's processing of Developer Personal Data.

11. Deletion and return

11.1 When the Terms end, or when Developer asks, Invo will delete or return Developer Personal Data, at Developer's choice, within ninety (90) days, and will delete existing copies, except where Applicable Data Protection Law or other law requires Invo to keep it.

11.2 Data that Invo keeps under a legal requirement remains protected by this DPA and is processed only for the purpose that requires it. Data in backups is deleted when the backups expire in the ordinary course.

11.3 Data for which Invo is an independent controller under Section 2.2 is not Developer Personal Data and is handled under Invo's Privacy Policy.

12. Audits

12.1 Invo will make available to Developer, on written request and no more than once a year, the information reasonably needed to demonstrate compliance with this DPA, which may include a summary of Invo's security measures, completed security questionnaires, and third-party audit reports or certifications Invo holds at the time.

12.2 Where that information is not sufficient to demonstrate compliance, or where a supervisory authority requires it, Developer may conduct an audit, at its own cost, by an independent auditor bound by confidentiality, on at least thirty (30) days' written notice, during normal business hours, in a way that does not disrupt Invo's operations or compromise the security of other customers' data. Remote audits are preferred.

13. Liability and order of precedence

13.1 Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Terms (Section 14), or in the parties' separate signed commercial agreement where one applies, except where Applicable Data Protection Law does not allow liability to be limited.

13.2 If this DPA conflicts with the Terms, this DPA controls for the processing of Developer Personal Data. If the SCCs apply, they control as stated in Section 7.3.

14. Term

This DPA lasts for as long as Invo processes Developer Personal Data under the Terms, and survives termination of the Terms for so long as Invo keeps any Developer Personal Data.

Schedule 1. Description of the processing

|---|---|

Parties	Controller (data exporter): Developer, as identified in its INVO Developer account. Processor (data importer): Invo Tech, Inc., Florida, United States.
Data subjects	Players of Developer's Games; Developer's own staff who use the Developer dashboard on Developer's behalf.

Categories of personal data	Player identifiers that Developer assigns; name, email address and phone number provided by Developer or the Player; Game-specific transaction events that Developer sends to the Platform; in-Game purchase, item and subscription records; loyalty and gameplay events that Developer sends; device and technical data relating to Game-specific requests; support communications about Developer's Game.
Sensitive data	None intended. Developer must not send special categories of personal data to the Platform.
Nature of processing	Collection, recording, storage, organization, retrieval, use, transmission to Developer (including by webhook), restriction and deletion.
Purposes	Operating the Platform features Developer uses for its Game: player records, Virtual Currency balances and transactions within the Game, item purchases, subscriptions, loyalty programs, webhooks and reporting to Developer, and customer support for Developer.
Frequency	Continuous, for as long as Developer uses the Platform.
Duration and retention	For the term of the Terms, then deleted or returned under Section 11, except where the law requires longer retention.
Subprocessor transfers	To the Subprocessor categories in Section 6.1, for the same purposes and duration.
Competent supervisory authority	The authority of the EU member state where Developer is established or, if Developer is not established in the EU, the Irish Data Protection Commission; for the UK, the Information Commissioner's Office; for Switzerland, the Federal Data Protection and Information Commissioner.
Technical and organizational measures	As set out in Section 5.

--- END OF DATA PROCESSING ADDENDUM ---