

TapMind Demand Partner Data Terms

Version 1.0, dated 1 October 2026

These Terms form part of the agreement between TapMind Asia Pacific Pte Ltd ("TapMind") and the demand partner identified in that agreement ("Partner") and govern personal data in bid requests TapMind sends from any Digital Property (websites, mobile apps, connected-TV/OTT, pre-installed and audio apps) and bid responses Partner returns ("Request Data" and "Response Data"). Capitalised terms not defined have the meanings in the agreement or Applicable Data Protection Law.

1. Roles

- 1.1** TapMind and Partner are independent controllers of Request Data. Neither determines the purposes or means of the other's processing. Each is responsible for its own legal basis, notices and compliance.
- 1.2** Nothing in these Terms makes either party the processor or agent of the other.

2. Permitted purposes and restrictions

- 2.1** Partner shall process Request Data only to decide whether and how much to bid, to serve, render, measure and frequency-cap the ad it bids on, to detect and prevent fraud and invalid traffic, and for aggregated internal analysis that does not identify an individual, device or publisher.
- 2.2** Partner shall not use Request Data to build or enrich profiles of end users, to identify or contact end users, to link any identifier to a persistent identifier, to fingerprint devices, or to sell, licence or disclose Request Data to any third party other than its processors bound by written terms no less protective, or as required by law.
- 2.3** Partner shall promptly delete Request Data relating to impressions it does not win, and shall retain Request Data relating to impressions it wins only as long as necessary for the permitted purposes.
- 2.4** Partner acknowledges TapMind never sends precise geolocation, hardware identifiers (including device serial numbers and MAC addresses), user-provided data or third-party identifiers, on any property type, and shall not require them.

3. Privacy signals

- 3.1** Partner shall honour every privacy signal accompanying a request, including IAB TCF consent and vendor status, IAB GPP section flags, the US Privacy string, `lmt`, `coppa` and any age or restricted-processing flags, and shall not process personal data where the signals do not permit its processing.
- 3.2** Partner shall maintain registration on the IAB Europe Global Vendor List for as long as it receives requests relating to EEA, UK or Swiss users, and shall be an IAB MSPA signatory or otherwise contractually bound to TapMind's satisfaction for US requests.
- 3.3** Partner shall support the IAB DSA transparency extension and return required transparency data for EU requests marked as requiring it.

- 3.4** Partner shall not bid on requests marked child-directed unless it processes no identifier and has demand suitable for children.
- 3.5** Partner shall comply with the TapMind Demand Partner Policies at tapmind.com/legal/demand-partner-policies.

4. Transfers

- 4.1** For Request Data relating to EEA users, the parties incorporate the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914), Module One, with Clause 7 included, Clause 17 law Ireland, Clause 18 forum Ireland, Annexes completed by Schedule A; the UK International Data Transfer Addendum for UK data; and the Swiss amendments for Swiss data.
- 4.2** Partner acknowledges that TapMind processes Request Data in India through its affiliate under contractual safeguards.
- 4.3** For other jurisdictions, each party ensures its own transfer compliance.

5. Individuals' rights and cooperation

- 5.1** Each party responds to requests concerning its own processing and forwards requests concerning the other within five business days.
- 5.2** Partner shall act on deletion or withdrawal requests forwarded by TapMind within 30 days and confirm completion on request.
- 5.3** Each party shall cooperate reasonably with the other's regulatory inquiries and, on request not more than once a year, provide information reasonably necessary to demonstrate compliance with these Terms.

6. Security and breach

- 6.1** Each party shall implement appropriate technical and organisational measures.
- 6.2** Each party shall notify the other without undue delay of a personal-data breach affecting Request Data or Response Data and cooperate in remediation and notifications.

7. Suspension

- 7.1** TapMind may suspend or restrict traffic to Partner immediately where Partner breaches section 2 or 3 or where TapMind reasonably believes continued traffic would breach Applicable Data Protection Law, and shall notify Partner of the reason.

8. Changes, liability, term

- 8.1** TapMind may update these Terms on 30 days' notice; Partner may terminate the affected services if an update materially reduces its rights.

- 8.2** Each party's liability under these Terms is subject to the limitations in the agreement.
- 8.3** These Terms survive for as long as either party holds Request Data or Response Data.
- 8.4** Electronic signature accepted; governing law as in the agreement save that the Standard Contractual Clauses are governed as stated in section 4.

Schedule A (Details of the transfer): parties (Partner as importer, TapMind Asia Pacific Pte Ltd as exporter for EEA data received from publishers under Module One); data subjects: end users of publishers' Digital Properties (websites, mobile apps, connected-TV/OTT apps, pre-installed apps, streaming-audio apps); categories: property and placement data, session, install or viewer identifiers, device and browser characteristics, IP and coarse location, consent signals, resettable advertising identifier (mobile, CTV, streaming-device) with its type where permitted, ad outcomes; no special categories; frequency: continuous; retention per section 2.3; competent authority per GDPR. **Schedule B** (technical and organisational measures): conventional list (access control, encryption in transit and at rest, logging, incident response, personnel confidentiality, sub-processor flow-down).