

TapMind Demand Partner Policies

Version 1.0, effective 1 October 2026

These Policies apply to every advertising partner receiving bid requests from TapMind for any Digital Property ("Partner"). They form part of the Partner's data terms with TapMind Asia Pacific Pte Ltd. TapMind may update them on 30 days' notice; versions at tapmind.com/legal/demand-partner-policies.

1. Use of request data

- 1.1** Partner may use data received in a bid request (from any Digital Property type, including websites, mobile apps, connected-TV/OTT, pre-installed and audio apps) only to decide whether and how much to bid, to serve, measure and cap the resulting ad, to detect fraud, and for aggregated internal analysis that does not identify a user or a publisher.
- 1.2** Partner must not use request data to build or enrich user profiles for any purpose other than serving the ad it bids on, unless the user's consent signals received with the request permit it and Partner's own privacy notice discloses it.
- 1.3** Partner must promptly delete request data for impressions it does not win, and in any event within any period specified in its data terms with TapMind, and must not retain identifiers beyond the period necessary for the permitted uses.
- 1.4** Partner must not sell, licence, or otherwise disclose request data to third parties except its own processors and as required by law.
- 1.5** Partner must not attempt to re-identify a user, link any advertising identifier (mobile, CTV, streaming-device or browser-based) to a persistent identifier, or fingerprint devices or browsers from request data.

2. Privacy signals

- 2.1** Partner must honour every privacy signal received with a request: IAB TCF consent and vendor status, GPP section flags, US Privacy string, `1mt`, `coppa`, and any age or restricted-processing flags, on every property type; where a request carries no consent signal from a jurisdiction that requires one, Partner must not process identifiers for personalised advertising.
- 2.2** Partner must be registered on the IAB Europe Global Vendor List to receive EEA, UK or Swiss requests carrying personal data, and must be an IAB MSPA signatory or otherwise contractually bound to receive US requests where TapMind requires it.
- 2.3** Partner must not bid for, or process, requests marked as child-directed unless it has child-safe demand and processes no identifier.
- 2.4** Partner must support the IAB DSA transparency signals and return the required transparency data for EU requests marked as requiring it.

3. Creative and content

- 3.1** Creatives must comply with the app platforms' policies, must not auto-redirect, auto-download, request permissions, collect data beyond what the winning response permits, or use undisclosed tracking.
- 3.2** Creatives must not contain malware, deceptive content, or content illegal in the impression's market.
- 3.3** Partner must provide creative metadata (advertiser domain, categories) on request.

4. Attribution and postbacks

- 4.1** Postback data exchanged for attribution may be used only for attribution and fraud detection, under the consent signals in force for the underlying impression.

5. Security, records, cooperation

- 5.1** Partner must maintain reasonable security measures, notify TapMind without undue delay of a breach affecting request data, and cooperate with TapMind's regulatory and publisher inquiries.
- 5.2** Partner must respond to deletion requests forwarded by TapMind within 30 days.

6. Enforcement

- 6.1** TapMind may throttle, suspend or remove Partner from any or all traffic for breach, and may do so immediately for privacy-signal violations, child-safety violations, or malicious creatives.