TapMind Demand Partner Policies

Version 1.0. Effective 5 November 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 the TapMind company it has contracted with (the "TapMind Entity"), which acts for TapMind Technologies Private Limited. 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, 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 delete request data for impressions it does not win promptly, and within any period specified in its data terms, 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, and must impose these Policies on anyone to whom it discloses request data.

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.

1.6 Where a request carries approximate location, Partner may use it only to select and measure the ad; Partner must not attempt to refine it, combine it with other location data to locate the user more precisely, or infer visits to sensitive places from it.

2. Privacy signals and frameworks

2.1 Partner must honour every privacy signal received with a request: IAB TCF consent and vendor status, GPP section flags, the US Privacy string, limit-ad-tracking, child-directed 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 To receive requests from the EEA, United Kingdom or Switzerland that carry personal data, Partner must be registered on the IAB Europe Global Vendor List and consented or permitted under the request's consent string.

2.3 To receive requests from the United States, Partner must be a signatory to the IAB Multi-State Privacy Agreement listed on its identification list, or must have accepted equivalent terms in writing with TapMind; where a request indicates that the consumer has opted out of sale, sharing or targeted advertising,

Partner must limit its processing to the activities the Agreement permits for opted-out consumers and must not use the advertising identifier for profiling or combine the request data with other data.

2.4 Partner must not bid for, or process, requests marked as child-directed unless it has child-safe demand and processes no identifier.

2.5 Partner must support the IAB DSA transparency signals and return the required transparency data for EU requests marked as requiring it.

2.6 Partner must preserve the supply chain object TapMind sends and must not remove, alter or re-order its nodes.

3. Creatives

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, write to device or browser storage, or use undisclosed tracking.

3.2 Creatives must not contain malware, deceptive content, or content illegal in the impression's market.

3.3 TapMind's SDK may fetch and hold a winning creative in the device's cache for up to 24 hours before display; impression, viewability and other event URLs must fire only on display, and creatives must not embed identifiers that outlive the impression.

3.4 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, deletion, 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 act on deletion requests TapMind forwards, including requests received through the IAB Data Deletion Request Framework, within 30 days or the shorter period the applicable law or framework requires.

5.3 Partner must notify TapMind if it can no longer meet these Policies.

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.