

TapMind Publisher Policies

Version 1.0, effective 1 October 2026

These Policies apply to every publisher using TapMind's Services (our SDKs, advertising tags, ad server, video player and platform) on any Digital Property: a website, mobile app, connected-TV or streaming (OTT) app, app pre-installed on a device, streaming-audio or podcast app, or digital out-of-home screen ("you"). They form part of your agreement with the TapMind Entity. TapMind may update them on 30 days' notice; the current and prior versions are at tapmind.com/legal/publisher-policies.

1. Privacy notice and consent

- 1.1** You must maintain a publicly accessible privacy policy for each Digital Property that discloses TapMind's identity and role, the categories of data the Services collect for that type of property, the purposes, the advertising partners enabled, and how users can exercise their choices, using the disclosure text TapMind provides (or its equivalent).
- 1.2** Where the law of a user's country requires consent for advertising identifiers, cookies, local storage or personalised advertising, you must obtain it before the related features operate, through a consent management platform that supports the applicable IAB framework and lists TapMind and each enabled partner as vendors, or through your own notice passed to TapMind via the Services' consent interfaces.
- 1.3** Where the Services are integrated through advertising tags in your ad server or other systems, you must configure those systems to populate TapMind's consent and privacy-signal parameters on every request.
- 1.4** You must never alter, suppress, spoof or delay the privacy signals your users or the device, browser or app platform set, and you must not use any feature in a way that circumvents a user's choice.
- 1.5** You must keep consent records where the law requires (time, text shown, mechanism) and make them available to TapMind on request in connection with a regulatory inquiry.

2. Identifiers and data transmitted to TapMind

- 2.1** You must transmit to TapMind only the data described in the Data Processing Addendum for the relevant property type.
- 2.2** On tag-based properties (websites, CTV/OTT, pre-installed and audio apps), you must configure your systems to pass only resettable advertising identifiers with their type, and never serial numbers, MAC addresses, hardware identifiers, precise geolocation, or user-provided data; identifiers may be passed only where the user's choices and the law permit.
- 2.3** You must not inject identifiers, user data or tracking parameters into TapMind's requests or creatives.

3. Platform, store and inventory compliance

- 3.1** You must keep your Google Play Data Safety section, Apple privacy labels and any equivalent platform disclosures accurate for the Services using the mapping TapMind provides, and update them within 30 days of a release that changes the mapping.
- 3.2** You must comply with Google Play's Ad ID policy, Apple's App Tracking Transparency requirements, and the advertising-identifier policies of each TV, streaming or device platform you distribute on, including honouring resets and limit-ad-tracking settings and never linking an advertising identifier to a persistent identifier.
- 3.3** You must maintain accurate ads.txt (websites), app-ads.txt (apps, including CTV/OTT and audio apps) and sellers.json entries authorising TapMind and its partners, and keep app bundle identifiers, store URLs and `ifa_type` values accurate in the inventory you make available.

4. Children and age-sensitive properties

- 4.1** You must accurately declare on the TapMind platform whether each Digital Property is directed at children, enrolled in Google Play's Families program, Apple's Kids category or an equivalent platform program, or likely to be used by a significant number of users under the age of majority in its principal markets, and update the declaration within 30 days of any change.
- 4.2** You must set the device, browser or app platform's child-directed and under-age-of-consent flags where applicable, and pass them through your ad server on tag-based properties.
- 4.3** On child-directed properties TapMind serves contextual advertising only; you must not attempt to enable identifier features for them.
- 4.4** If a regulator or platform determines your property is child-directed, you must notify TapMind within 30 days.

5. Use of the Services software

- 5.1** You may use the SDKs, tags, ad server integrations and video player only as documented; you must not modify, reverse-engineer or bypass them, extract or persist identifiers from them, or use them on any property other than those registered on the platform.
- 5.2** You must stay within supported versions and apply security updates within 90 days of release.
- 5.3** You must not use the Services to collect data TapMind does not collect.

6. Prohibited content and traffic

- 6.1** You must not use the Services on properties that are illegal in their distribution markets, that infringe third-party rights, that contain or promote hate, violence, sexual content involving minors, or that mislead users.
- 6.2** You must not generate invalid traffic (bots, undisclosed incentivised interactions, click farms, forced or deceptive ad interactions, hidden or stacked ads, auto-refresh beyond permitted limits, spoofed apps,

devices or inventory).

- 6.3** You must not misrepresent inventory (for example, declaring web inventory as CTV, or a mobile web page as an app).
- 6.4** TapMind may withhold payment for invalid or misrepresented traffic under the Agreement.

7. Attestation and cooperation

- 7.1** You must complete and confirm the platform attestation truthfully for each Digital Property and keep it current.
- 7.2** You must forward user requests concerning TapMind within five business days and cooperate with TapMind in responding to regulatory inquiries.
- 7.3** You must notify TapMind promptly of any complaint or inquiry that concerns TapMind's processing.

8. Enforcement

- 8.1** Breach of these Policies is a breach of the Agreement. TapMind may apply the enforcement ladder in section 9, up to suspension or termination, and may report invalid traffic to industry bodies.
- 8.2** Where the breach is a privacy-notice, consent or identifier-transmission failure, TapMind may disable identifier features for, or stop serving, the affected properties immediately and without liability.

9. Enforcement ladder

Notice and 14 days to cure → identifier features disabled for the affected properties → property suspended → publisher account suspended → termination. TapMind may skip steps for invalid traffic, misrepresented inventory, children-safety violations, or legal exposure.