

TapMind Privacy Policy

Version 1.1, effective 8 November 2026

In short. TapMind provides advertising technology to publishers of websites, mobile apps, connected-TV and streaming apps, pre-installed apps, audio apps and digital screens. When you use one of these properties and it requests an ad through TapMind, we process limited information about your browser or device and how ads perform there, so that ads can be shown, measured and paid for. Where the law requires your consent (for example, to use your device's advertising identifier to personalise ads, or to store information in your browser), we or the property's publisher will ask for it, and you can withdraw it at any time. We never collect your name, contact details, precise location, or any hardware identifier that cannot be reset. You can ask us what we hold about your device and ask us to delete it at privacy@tapmind.com.

1. Who we are and what this policy covers

"TapMind", "we" and "us" means the TapMind group: **TapMind Asia Pacific Pte Ltd** (UEN 202642669W, 68 Circular Road, #02-01, Singapore 049422) and **TapMind Technologies Pvt Ltd** (CIN U72200KA2015PTC083215, Zed Pentagon, 4th Floor, NGR Layout, Roopena Agrahara, Bommanahalli, Bengaluru, Karnataka 560068, India). TapMind's advertising technology, being our software development kits ("SDKs"), advertising tags, ad server, video player and platform (together, the "Services"), is developed and operated by TapMind Technologies Pvt Ltd on behalf of the group.

This policy applies when you use a **Digital Property** whose publisher uses our Services to show ads: a website, a mobile app, a connected-TV or streaming (OTT) app, an app pre-installed on a device by its manufacturer, a streaming-audio or podcast app, or a digital out-of-home screen. It does not cover the publisher's own collection of your data, or our own website, which has its own cookie notice at tapmind.com/legal/cookies.

Which TapMind entity is responsible for your data (the "controller", "data fiduciary" or "organisation" in the language of your local law) depends on the Digital Property you are using: TapMind Asia Pacific Pte Ltd is responsible where the publisher has contracted with it, which includes most Digital Properties outside India; TapMind Technologies Pvt Ltd is responsible where the publisher has contracted with it, which includes most Digital Properties in India. If you are unsure, write to us and we will tell you. Both entities apply this policy in full, and both can be reached at the contacts in section 12.

2. What we collect

When a Digital Property requests an ad through our Services, we receive some or all of the following, depending on the type of property and on what its publisher's systems send us:

- **Property and ad-placement information:** the identifier of the website, app or channel, the app version, the ad slot with its placement code and name, ad format and size, the page or content context, which advertising partners the publisher uses, and the version of our software.
- **Identifiers that recognise your browser or device:** described by property type below. We never receive your name, email address, phone number or account details.
- **Device and browser characteristics:** device make and model, device type, operating system and version, browser type, screen size, language, connection type, carrier name and network code, and time-zone

offset. In mobile apps, where the publisher has enabled it, we also receive coarse information about the state of the device and the app: for example whether the battery is low, how much memory and storage are free, the quality of the network connection, and how often the app has been opened. These values are grouped into broad ranges on your device before they are sent. We use them only to make our Services work better and to detect fraud. We never send them to advertising partners, and we never combine them to create an identifier.

- **Network information:** your IP address, which we use to determine your country and, where permitted, your region or city. We do not keep your full IP address beyond short-lived security logs.
- **Consent and privacy signals:** the choices you have made in the property's consent dialog or in your device or browser settings (for example, IAB TCF or GPP strings, "limit ad tracking", App Tracking Transparency status), and any age-related flags the publisher or its ad platform sets.
- **Ad outcomes:** whether an ad was requested, loaded, shown or clicked, how long it took, any error, and the revenue reported for it.

How we recognise your browser or device on each type of property

- **Mobile apps that include our SDK:** a random session identifier that changes when you stop using the app for a period; a random install identifier created by our SDK on your device that changes if you reinstall the app and is never derived from, or linked on your device to, any other identifier; and, only where the publisher has enabled the feature, the law of your country permits it, you have not limited ad tracking or opted out, and you have given consent where consent is required, your device's advertising identifier (Google Advertising ID on Android; IDFA on iOS). We never use the advertising identifier in apps directed at children.
- **Websites:** our advertising tag and video player do not set cookies. They store a small amount of information in your browser's local storage and session storage, such as a random viewer identifier used to limit how often you see the same ad and to record your privacy choices; the items, their purposes and how long they last are listed in our Platform Cookie & Similar Technologies Policy at tapmind.com/legal/platform-cookies.
- **Connected-TV, streaming, pre-installed and audio apps:** the publisher's ad server sends us, where it is configured to do so, the device's resettable advertising identifier (for example a Roku, Fire TV, Samsung, LG, Android TV or Apple TV advertising ID) and its type, together with the app, channel or content context. We receive only what the publisher's systems transmit through our tags, and we do not process device serial numbers, MAC addresses or other hardware identifiers on any device.
- **Digital out-of-home screens:** we receive no information about individuals from screens. Where a screen owner supplies audience estimates, they are aggregate and do not relate to you.

We never collect: your name, email, phone number or contacts; precise (GPS) location; hardware identifiers such as IMEI, serial number or MAC address; a list of apps on your device; or the contents of your device. We do not create "fingerprints" from device or browser characteristics to identify you.

3. Why we use it

Purpose	What it means	Data used
Serving ads and choosing between ad sources	Deciding which advertising partner is likely to fill an ad slot and at what value	Property, placement, install or viewer identifier, device characteristics, ad outcomes

Purpose	What it means	Data used
Reporting to publishers and reconciliation	Telling publishers how their ads performed and settling payments	Aggregated property, device-type and outcome data, never individual-level reports
Limiting how often you see an ad on a property	Frequency capping within one Digital Property	Install or viewer identifier, ad outcomes
Sending ad requests to advertising partners	Asking partners for a bid on an ad slot	Property, placement, device characteristics, consent signals, country and (where permitted) region/city, and the advertising identifier where permitted
Recognising your device across apps	Limiting how often you see an ad across apps, and measuring reach	Advertising identifier (only with consent where required)
Personalised advertising	Building audience segments and showing ads that are more relevant to you	Advertising identifier and ad-interaction history (only with consent where required)
Attribution	Telling an advertiser that an install or action came from an ad	Advertising identifier and click/impression records, sent to the advertiser's measurement partner (only with consent where required)
Our own advertising campaigns	Running campaigns for TapMind or its direct advertisers under the same rules	As above, per purpose
Security, fraud prevention and legal compliance	Detecting invalid traffic, keeping records the law requires, responding to requests	Any of the above, as needed

4. Legal bases

Where your law requires a legal basis, we rely on:

- **Your consent** for the advertising identifier, cross-property recognition, personalised advertising and attribution, and for storing or reading identifiers on your device or in your browser where that requires consent (for example, in the EEA and UK). Where a Digital Property does not pass us a consent signal, we and our partners treat that as no consent for these purposes and serve non-personalised ads. You can withdraw consent at any time (section 8).
- **Our legitimate interests** (or the equivalent basis in your law) in operating, securing and improving our advertising service, for ad serving, source selection, frequency capping within a property, reporting, and fraud prevention, where those interests are not overridden by your rights. A summary of these interests, how we balance them against your rights, and how to object is at tapmind.com/privacy/legitimate-interests. Where your law does not provide such a basis for these activities (for example, India), we rely on consent obtained through the notice of the Digital Property you are using.
- **Legal obligation**, for records we must keep and requests we must answer.

In markets with an opt-out model (United States), we process as described unless you opt out of the sale or sharing of your information or of targeted advertising (section 13).

5. Who we share it with

- **Advertising partners** that bid on ad slots. They receive the request information in section 3 ("Sending ad requests") and act as independent controllers under their own privacy policies. We forward the consent and privacy signals we receive with each request, and partners may only use your data where those signals permit. Where a partner cannot honour your choices, we do not send it your request.
- **Attribution and measurement partners** designated by advertisers, for attribution (with consent where required).
- **Google**, where the Digital Property uses Google's ad platforms; Google's own policies apply to its processing.
- **Infrastructure providers**: cloud, hosting, content-delivery, database, security and messaging providers that host and operate our systems, listed with their locations at tapmind.com/legal/subprocessors.
- **Publishers** receive aggregated reports about their own Digital Properties, never individual-level data.
- **Authorities**, where the law requires.

We do not sell personal information for money. In some US states, sending information to advertising partners is treated as a "sale" or "sharing"; you can opt out (section 13).

6. Where we process it

Our systems are hosted primarily in India. We may also use infrastructure operated by us or our infrastructure providers in other countries, including the United States and the European Union, where that helps us serve ads closer to you or meet our customers' needs; the current providers and locations are listed at tapmind.com/legal/subprocessors. Wherever your data is processed, we apply the safeguards your law recognises: the European Commission's Standard Contractual Clauses with a transfer impact assessment (EEA), the UK Addendum (UK), the Swiss addendum (Switzerland), the Standard Contractual Clauses approved by the Saudi Data & AI Authority (Saudi Arabia), and contractual protections meeting the standard of Singapore's Transfer Limitation Obligation and comparable laws elsewhere. In countries whose law requires personal data to stay in the country, we do not store any identifier linked to your device (section 16).

7. How long we keep it

We keep personal data only as long as needed for the purposes above, and no longer than the periods below, unless the law requires us to keep it longer.

Data	Kept for
Advertising identifier	Up to 13 months from the last time we saw it, or until you withdraw consent, reset it, or ask us to delete it, whichever is first
Install identifier and the profile linked to it	Up to 24 months from the last activity, or until deletion
Records of your consent choices	Up to 5 years after withdrawal or deletion, as evidence
Ad-serving logs (pseudonymised)	Up to 13 months
Security logs containing IP addresses	Up to 30 days; the IP address is masked after 7

Data	Kept for
Aggregated reporting	Indefinitely, because it does not identify you

8. Your choices

- **Mobile apps:** in your device settings, delete or reset your advertising ID (Android) or decline App Tracking Transparency (iOS), which we honour immediately; or change your choices in the app's consent dialog, which passes them to us on your next ad request; or, where we show our own consent screen, reopen it from the app's privacy settings.
- **Websites:** use the consent dialog on the website you are visiting; opt out of personalised advertising by TapMind at tapmind.com/privacy/choices, which stores your choice in your browser; or clear your browser's site data, which removes anything we have stored. Choices are stored per browser, so repeat them on each browser you use.
- **Connected TVs, streaming devices and audio apps:** use your device's advertising settings to limit ad tracking or reset the advertising identifier (for example the Advertising section under Privacy on Roku, or the Ads section under Privacy on Fire TV, Google TV and Apple TV); the Network Advertising Initiative maintains step-by-step instructions by device at thenai.org. You can also submit your device's advertising identifier at tapmind.com/privacy/choices.
- **Our privacy-choices page** at tapmind.com/privacy/choices: opt out of personalised advertising, or ask us to delete or show the data we hold for your browser or device, using your advertising, installation or viewer identifier.
- **Write to us** (section 12) to withdraw consent, object, or opt out.

Because different devices and browsers use different identifiers, opt-outs apply to the device or browser on which you make them. Withdrawing consent stops the related processing going forward; it does not affect processing before withdrawal.

9. Your rights

Depending on your law, you may have the right to access the information we hold about your device, to correct it, to delete it, to restrict or object to processing, to portability, to withdraw consent, to opt out of sale, sharing or targeted advertising, not to be discriminated against for exercising rights, and to complain to a supervisory authority. To exercise a right, contact us (section 12). Because we hold no name or contact details, we identify your data by the install or viewer identifier (shown in the app's privacy settings, obtainable from the publisher, or stored in your browser) or your device's advertising identifier (shown in your device settings). We respond within the time your law sets (generally one month in the EEA and UK, 45 days in the United States, 30 days in Singapore and Canada, and within 90 days in India), and usually much sooner.

10. Children

We do not knowingly process the personal data of anyone under 18 for targeted advertising, and we do not sell or share such data. We do not offer our Services to mobile apps that are directed at children, that include children in their declared audience, or that are included in Google Play's Families program or Apple's Kids category. On other Digital Properties that are directed at children, or flagged as child-directed by the publisher or its ad platform, we use no advertising identifier and show only contextual ads. Where a request from a mobile app tells us that it relates to a child, or to a user under the age of majority in their country, we do not show an ad and we use no

advertising identifier. On other Digital Properties we use no advertising identifier for such a request and show only contextual ads. If you believe we have collected data from a child, contact us and we will delete it.

11. Security

We use encryption in transit and at rest, field-level encryption for advertising identifiers, strict access controls with no routine human access to identifiers, pseudonymisation of serving logs, and audit logging of privileged actions. No system is perfectly secure; if a breach affecting you occurs, we will notify you and the relevant authority as your law requires.

12. Contact

Privacy requests: privacy@tapmind.com. Grievances (India) and Data Protection Officer: Naveen Chennala, Director, privacy@tapmind.com, Zed Pentagon, 4th Floor, NGR Layout, Roopena Agrahara, Bommanahalli, Bengaluru, Karnataka 560068, India. Singapore Data Protection Officer: Naveen Chennala, Director, privacy@tapmind.com.

13. Additional information for United States residents

Categories collected in the last 12 months: identifiers (install and advertising identifiers), internet or network activity (ad interactions), device information, coarse geolocation, and inferences (audience segments where personalisation is enabled). Sources: the website, app or channel you use, and its publisher's systems. Business purposes: section 3. Categories disclosed to advertising partners for advertising purposes ("sale"/"sharing"/"targeted advertising"): identifiers, device information, coarse geolocation, ad interactions. We do not use or disclose sensitive personal information, and we do not knowingly sell or share information of consumers under 18. You may opt out of sale, sharing and targeted advertising through the app's privacy choices, at tapmind.com/privacy/choices, by using the Global Privacy Control where the property you are using supports it, or by contacting us. To submit a request to know, delete or correct your information, use the form at tapmind.com/privacy/choices or email privacy@tapmind.com. We have not sold or shared the personal information of consumers we know to be under 18. We honour opt-out preference signals as required by your state's law. You will not be discriminated against for exercising your rights. Authorised agents may act on your behalf with written permission.

14. Additional information for India

This notice is given under the Digital Personal Data Protection Act, 2023. The data fiduciary is the TapMind entity identified in section 1. We process your personal data for the purposes in section 3 on the basis of your consent, given through the notice of the website, app or channel you are using or TapMind's own notice, which you may withdraw as easily as you gave it (section 8), and for legitimate uses permitted by the Act. We do not track, behaviourally monitor, or direct targeted advertising at children. You may access, correct, update or erase your personal data, nominate a person to exercise your rights, and raise grievances with our Grievance Officer (section 12), who will respond within the time prescribed. If your grievance is not resolved, you may approach the Data Protection Board of India.

15. Additional information for the EEA, United Kingdom and Switzerland

TapMind will register with the IAB Europe Transparency & Consent Framework before serving personalised advertising in these regions. Until that registration is complete, TapMind serves only contextual advertising in the EEA, UK and Switzerland and does not process advertising identifiers there. Once registered, our vendor ID, declared purposes and legal bases will be listed in the Global Vendor List and on this page. Storing or reading identifiers on your device or in your browser is done only with your consent, except where strictly necessary. TapMind does not currently serve advertising to users in the EEA, the United Kingdom or Switzerland; if we begin to, we will appoint representatives in the EU and the UK and list them in section 12. You may lodge a complaint with your national data protection authority or the ICO.

16. Additional information for other countries

Canada: we rely on your meaningful consent obtained through the website or app you are using; in Quebec, technologies that identify, locate or profile you are off by default until you turn them on; you may complain to the Office of the Privacy Commissioner or the Commission d'accès à l'information. **Singapore:** our Data Protection Officer is listed in section 12; we rely on consent, deemed consent by notification, or the legitimate interests exception, as described in section 4. **Saudi Arabia:** transfers outside the Kingdom use SDAIA's standard clauses. **Indonesia:** we rely on consent and legitimate interest as permitted by Law No. 27 of 2022. **Countries requiring data to remain in-country:** we do not store any identifier linked to your device.

17. Publishers, partners and business contacts

If you are a contact at a publisher, advertising partner or supplier, we process your business contact details to manage our relationship, under contract or legitimate interest, and keep them for the life of the relationship plus the period required by law.

18. Changes to this policy

We version this policy. The current version and all previous versions are available at tapmind.com/privacy. Material changes are announced on that page at least 30 days before they take effect, and publishers are notified so they can inform you.