TapMind Data Processing Addendum

Version 1.0. Dated 5 November 2026

This Data Processing Addendum ("**DPA**") forms part of the agreement between the Publisher and the TapMind Entity for the provision of TapMind's advertising technology services (the "**Agreement**"). This DPA is attached to the Agreement as a schedule; a copy is also published at tapmind.com/legal/dpa/v1.0 for reference only. In the event of any difference, the copy attached to the Agreement governs.

1. Definitions and precedence

1.1 "**Controller**" means TapMind Technologies Private Limited, a company incorporated in India (CIN U72200KA2015PTC083215), which determines the purposes and means of the Processing of Service Data and is the controller, data fiduciary or organisation responsible for it under Applicable Data Protection Law. "**TapMind Entity**" means the party to the Agreement, being either the Controller or its affiliate TapMind Asia Pacific Pte. Ltd. (UEN 202642669W); where the TapMind Entity is TapMind Asia Pacific Pte. Ltd., it enters into the Agreement and this DPA for and on behalf of the Controller, and every obligation of "TapMind" in this DPA is an obligation of the Controller, performed by the Controller. "**TapMind**" means the Controller and, where the context requires, the TapMind Entity. "**Publisher**" means the other party to the Agreement. "**Personal Data**", "**Processor**", "**Data Subject**", "**Processing**" and "**Supervisory Authority**" have the meanings given in Applicable Data Protection Law and include their equivalents under each such law. "**Applicable Data Protection Law**" means every law that applies to the Processing of Personal Data under this DPA, including those listed in Schedule 5. "**Digital Property**" means each website, mobile application, connected-TV or streaming (OTT) application, application pre-installed on a device by its manufacturer, streaming-audio or podcast application, digital out-of-home screen, or other digital property registered by the Publisher on the TapMind platform or listed in the Agreement. "**Services**" means the TapMind SDK and its mediation adapters, advertising tags, ad server, video player, platform and related services, as used on a Digital Property. "**End User**" means a user of a Digital Property. "**Infrastructure Providers**" means the third parties that provide TapMind with cloud computing, hosting, storage, content delivery, networking, managed database, security, monitoring and messaging services, as listed at tapmind.com/legal/subprocessors. "**Service Data**" means Personal Data of End Users Processed through the Services, as described in Schedule 1. "**Purposes**" means the purposes in Schedule 2. "**Privacy Signal**" means any consent, opt-out, limit-ad-tracking, age or similar signal set by an End User, a device or app platform, or a consent management platform.

1.2 Schedules form part of this DPA. Schedule 5 modules apply only where stated.

1.3 This DPA prevails over the Agreement to the extent of any conflict concerning Personal Data. A Schedule 5 module prevails over this main body for the jurisdiction it covers.

2. Roles

2.1 **Independent controllers.** For the Purposes marked "TapMind: Controller" in Schedule 2, the Publisher and the Controller are each independent controllers of Service Data. Each determines its own purposes

and means and is separately responsible for its own compliance. Nothing in this DPA makes either party the Processor or agent of the other for those Purposes.

2.2 **Processor.** For the Purposes marked "TapMind: Processor" in Schedule 2, the Controller acts as Processor on behalf of the Publisher, and clause 6 applies.

2.3 **Joint control.** The parties do not intend to be joint controllers. If a Supervisory Authority or court determines that they are joint controllers of any Processing (including the collection of Service Data by the Services on a Digital Property), then, for that Processing only: (a) the Publisher is responsible for providing the notice and obtaining any consent required from End Users at the point of collection, in the form in Schedule 6; (b) the Controller is responsible for all Processing after collection; (c) each party is responsible for responding to Data Subject requests it receives and for its own security; and (d) the essence of this arrangement is made available to End Users through the parties' privacy notices.

2.4 **Contracting affiliate.** Where the TapMind Entity is TapMind Asia Pacific Pte. Ltd., the Publisher acknowledges that TapMind Asia Pacific Pte. Ltd. contracts as the agent of the Controller under a written intra-group agreement, that it does not itself Process Service Data, and that the Controller is responsible for the Processing of Service Data and for the performance of this DPA. Notices and requests under this DPA may be given to either TapMind company and are effective against the Controller.

3. Publisher's obligations

3.1 The Publisher shall comply with Schedule 6, including: (a) providing End Users with a privacy notice that identifies TapMind Technologies Private Limited as controller, the Purposes and the means to exercise rights, using the disclosure text TapMind provides or its equivalent; (b) where Applicable Data Protection Law requires consent, obtaining valid consent covering TapMind and the Purposes, through a consent management platform that supports the IAB frameworks where applicable, through the Publisher's own notice passed to TapMind through the SDK's consent interface, or by allowing TapMind to present its own notice where the Services provide one; (c) accurately completing and keeping current the attestation on the TapMind platform for each Digital Property, including its type, whether it is directed at or likely to be used by children, and whether it is an online platform under the EU Digital Services Act; (d) updating its app-store, platform and other disclosures (including Google Play Data Safety and Apple privacy labels where applicable) to reflect the Services, and, before approximate device location is enabled for a Digital Property, declaring that location is collected and shared for advertising; (e) passing to TapMind, without alteration, the Privacy Signals set by End Users and by the device or app platform; (f) where the Services are integrated through advertising tags in the Publisher's ad server or other systems, configuring those systems to populate TapMind's consent and Privacy Signal parameters, to transmit only resettable advertising identifiers (never serial numbers, hardware identifiers, precise geolocation or user-provided data), and to transmit identifiers only where End Users' choices and Applicable Data Protection Law permit; and (g) publishing and maintaining the app-ads.txt or ads.txt line TapMind issues for the Digital Property.

3.2 The Publisher warrants that it has the right to make Service Data available to TapMind for the Purposes, and shall not make available to TapMind any Personal Data other than Service Data, whether through the Services, through advertising tags, or otherwise. TapMind does not accept, and will discard, any information about an End User supplied by the Publisher that is not Service Data, such as age, gender or interests.

4. TapMind's obligations

4.1 The Controller shall Process Service Data only for the Purposes, in accordance with this DPA, its published privacy policy and Applicable Data Protection Law.

4.2 The Controller shall: (a) Process an End User's advertising identifier (or equivalent resettable device identifier) only where the Publisher has enabled that feature for the Digital Property after execution of this DPA and completion of the attestation, or transmits the identifier through the Services, Applicable Data Protection Law permits it, any required consent has been given and not withdrawn (in the EEA, UK and Switzerland, consent for storing and accessing information on the device and for creating and using profiles for personalised advertising, given to TapMind through a consent management platform), the End User has not limited ad tracking, opted out, or placed the identifier on TapMind's suppression list, and the Digital Property is not directed at children; (b) link an advertising identifier to install identifiers, or build a profile, only under the conditions in (a); (c) Process approximate device location only where the Publisher has enabled it for the Digital Property, the Publisher has made the declaration in clause 3.1(d), the application already holds the End User's permission to access location, and any required consent has been given, and only after the location has been reduced on the device to an area that is not precise; (d) honour every Privacy Signal it receives within the time stated in Schedule 1; (e) not collect precise geolocation, non-resettable device identifiers, contact information, or any data listed as "never collected" in Schedule 1, and not accept user-provided data; (f) not create device fingerprints; (g) not sell Personal Data for monetary consideration; (h) apply the retention periods in Schedule 1; (i) maintain the measures in Schedule 3; (j) store on End Users' devices and in their browsers only the items disclosed at tapmind.com/legal/storage-disclosure.json; and (k) for Service Data transmitted through advertising tags, Process only what the Publisher's systems transmit and apply the same Privacy Signal checks before any disclosure to partners as it applies to Service Data collected by the TapMind SDK.

4.3 The Controller shall disclose Service Data to advertising partners and attribution partners only as independent controllers bound by written terms requiring them to process Service Data only to bid, serve, measure and cap the advertisement concerned, to detect fraud, and for aggregated analysis; to honour End Users' Privacy Signals, passed to them unchanged; not to re-identify End Users, link identifiers to persistent identifiers, or fingerprint devices; to act on deletion requests forwarded by TapMind; to apply the same restrictions to anyone to whom they disclose the data; and to comply with Applicable Data Protection Law. The Controller shall not disclose Service Data to any partner that cannot honour a Privacy Signal applicable to the request, that is not registered under the IAB Europe Transparency and Consent Framework for requests from the EEA, UK or Switzerland, or that is neither a signatory to the IAB Multi-State Privacy Agreement nor bound by equivalent terms for requests from the United States. The partners are listed at tapmind.com/developers/privacy/partners.

5. Data Subject requests and complaints

5.1 Each party shall respond to Data Subject requests it receives concerning its own Processing. Where a request concerns the other party's Processing, the receiving party shall forward it within five business days and provide reasonable assistance. The Controller accepts requests identified by install identifier or advertising identifier, through tapmind.com/privacy/choices and privacy@tapmind.com, and provides a mechanism for the Publisher to submit erasure requests on End Users' behalf.

5.2 Each party shall notify the other promptly of any complaint or Supervisory Authority inquiry concerning the Services, to the extent lawful.

6. Processor terms (Schedule 2 "TapMind: Processor" Purposes only)

6.1 The Controller, acting as Processor, shall Process Personal Data only on the Publisher's documented instructions, which are the Agreement, this DPA and the Publisher's use of the platform; ensure persons authorised to Process are bound by confidentiality; implement Schedule 3; engage sub-processors only under clause 7; assist the Publisher, taking into account the nature of the Processing, in responding to Data Subject requests and in meeting its obligations regarding security, breach notification, impact assessments and prior consultation; at the Publisher's choice delete or return the Personal Data at the end of the Services, except where retention is required by law; and make available the information necessary to demonstrate compliance and allow audits under clause 9.

6.2 The Controller shall inform the Publisher if, in its opinion, an instruction infringes Applicable Data Protection Law.

7. Sub-processors

7.1 The Publisher authorises the sub-processors listed in Schedule 4, by category. The Controller shall impose on each sub-processor written obligations no less protective than this DPA and remains responsible for their performance.

7.2 The Controller shall give the Publisher 30 days' prior notice of any new or replacement sub-processor by updating tapmind.com/legal/subprocessors and notifying the Publisher's registered contact. The Publisher may object in writing on reasonable data-protection grounds within that period; the parties shall discuss in good faith and, if no resolution is reached within a further 30 days, the Publisher may terminate the affected Services without penalty.

8. Security and personal-data breach

8.1 Each party shall implement appropriate technical and organisational measures; TapMind's measures are in Schedule 3.

8.2 The Controller shall notify the Publisher without undue delay after becoming aware of a personal-data breach affecting Service Data, with the information reasonably required for the Publisher to meet its own notification obligations, and shall cooperate in remediation. Notification is not an admission of fault.

9. Audit and information

9.1 On written request not more than once per year (or following a breach or a Supervisory Authority request), the Controller shall complete a reasonable security and privacy questionnaire and provide relevant certifications, policies and summaries of independent assessments. Where these are insufficient to demonstrate compliance, the Publisher may conduct, or appoint an independent auditor bound by confidentiality to conduct, an audit at the Publisher's cost, on 30 days' notice, during business hours, without disrupting operations, and limited to Service Data Processing.

10. International transfers

10.1 The Controller Processes Service Data in India and at the locations listed at tapmind.com/legal/subprocessors. Each party shall ensure that any transfer of Personal Data under this DPA complies with Applicable Data Protection Law, using the mechanisms in the applicable Schedule 5 module. Where a module incorporates standard contractual clauses, the parties agree that executing the Agreement executes those clauses with the selections stated in the module, with the Controller as the data importer and the TapMind Entity, where it is not the Controller, signing on the Controller's behalf.

11. Retention and deletion

11.1 The Controller shall retain Service Data no longer than the periods in Schedule 1, and shall delete or irreversibly pseudonymise Service Data on expiry, on withdrawal of consent, on a valid erasure request, and on termination of the Agreement, save for records it is required by law to keep and evidence of consent choices and opt-outs.

12. Cooperation and impact assessments

12.1 Each party shall provide the other with reasonable assistance in carrying out data-protection impact assessments and consultations with Supervisory Authorities relating to the Services, and the Controller shall make its impact-assessment summary available on request.

13. Children

13.1 The Publisher shall accurately declare, and keep current on the TapMind platform, whether each Digital Property is directed at children, includes children in its declared audience, is enrolled in a child-focused app-store or platform program, or is likely to be used by a significant number of users under the age of majority in its principal markets. TapMind does not provide the Services to mobile applications in the first three categories, and may suspend the Services to any Digital Property it reasonably determines falls within them. For any request flagged as relating to a child, the Controller shall Process no advertising identifier and serve only contextual advertising, and shall not knowingly Process Personal Data of anyone under 18 for targeted advertising.

14. Liability and indemnity

14.1 This DPA does not alter the limitations and exclusions of liability set out in the Agreement, which apply to each party's liability under this DPA. Nothing limits liability that cannot be limited by law.

14.2 The Publisher shall indemnify and hold harmless TapMind against third-party claims, regulatory fines and penalties, and reasonable costs arising from the Publisher's failure to provide the privacy notice required by clause 3.1(a), to obtain or maintain any consent required by clause 3.1(b), to make the declaration required by clause 3.1(d), to declare accurately the matters in clause 3.1(c) and clause 13, or to pass End Users' Privacy Signals to TapMind without alteration as required by clause 3.1(e).

15. Changes to this DPA

15.1 This DPA is version-controlled. The version identified on its face governs the parties until replaced under this clause. TapMind may not change this DPA except: (a) where required by a change in Applicable Data Protection Law or a binding order, in which case it shall give the Publisher at least 30 days' notice (or such shorter period as the law requires) of the minimum change necessary, with the new version published to the register with a change note; (b) by updating Schedule 4 under clause 7; or (c) by the Publisher's written acceptance of a new version. A new version does not affect the Publisher until accepted under (a) or (c). All versions remain available at tapmind.com/legal/dpa with their dates and document hashes.

16. General

16.1 Term: this DPA applies for as long as the Controller Processes Service Data under the Agreement, and clauses 11 and 14 survive termination.

16.2 Governing law and venue: as in the Agreement, except where a Schedule 5 module requires otherwise.

16.3 This DPA may be executed by electronic signature, and the parties agree that an electronic signature satisfies any requirement for a signature under Applicable Data Protection Law.

16.4 Notices under this DPA go to the contacts registered on the TapMind platform and to privacy@tapmind.com.

Signed for the TapMind Entity (**[TapMind Technologies Private Limited | TapMind Asia Pacific Pte. Ltd., for and on behalf of TapMind Technologies Private Limited]**): Naveen Chennala, Director · for the Publisher: **[name, title]** · Date: **[date]**

Schedule 1 · Processing details

Particular	Detail
Subject matter	Serving, measuring and monetising digital advertising on Digital Properties through the Services
Duration	The term of the Agreement plus the retention periods below
Nature	Collection through the Services (SDK and adapters, tags, ad server, video player), receipt of data transmitted by the Publisher's systems, transmission, storage, analysis, disclosure to advertising and attribution partners, aggregation, deletion
Categories of Data Subjects	End Users of Digital Properties
Categories of Personal Data, by property type	See the table immediately below this schedule

Particular	Detail
Never collected	Name, contact details, account identifiers; user-provided attributes such as age, gender or interests; precise geolocation; IMEI, serial, MAC or other hardware identifiers; installed-app lists; device contents; biometric or special-category data; device or browser fingerprints; individual-level data from DOOH screens
Special categories	None; the Controller shall not infer special categories
Retention	No longer than necessary for the Purposes and, in any event, within the maximum periods stated in the TapMind privacy policy in force at the time of Processing (currently: advertising identifier and any links to install identifiers up to 12 months from last seen; install identifier and linked history up to 12 months from last activity; data used to select ads without a profile up to 3 months; pseudonymised ad-performance records up to 13 months; raw inputs for audience statistics up to 3 months and for service improvement up to 6 months; security, diagnostics and fraud logs up to 3 months with IP addresses masked after 7 days; consent and opt-out records up to 5 years after withdrawal, opt-outs for as long as needed to honour them). Aggregated reporting is not personal data and is retained indefinitely.
Location	The Infrastructure Providers and processing locations listed at tapmind.com/legal/subprocessors (at the date of this DPA: India). Additional providers or locations are notified under clause 7.2.
Signal honouring time	Withdrawal or opt-out is applied to the next ad request from the device or browser; linked identifiers are severed and erasure is completed promptly and within the periods required by Applicable Data Protection Law
Device storage	The items the Services store on devices and in browsers, with their lifetimes and purposes, are disclosed at tapmind.com/legal/storage-disclosure.json and at tapmind.com/legal/platform-cookies

Categories of Personal Data by property type (part of Schedule 1)

Category	Mobile apps (TapMind SDK)	Websites (tag, video player)	CTV/OTT, pre-installed and audio apps (tags)	DOOH
Property and placement context	App ID, app version, placement code and name, format, mediation platform, partners, SDK version	Site, page context, placement, format	App bundle, channel or content context, placement, format	Screen and placement
Identifiers	Install identifier; session identifier (memory only); advertising identifier (GAID/IDFA) under clause 4.2(a), read per request and not stored on the device; links between them under clause 4.2(b)	None. Browser local and session storage hold frequency counters, priority state, a configuration cache and an opt-out flag; no cookies and no identifier	Resettable device advertising identifier and its type, as transmitted by the Publisher's ad server under clause 3.1(f)	None

Category	Mobile apps (TapMind SDK)	Websites (tag, video player)	CTV/OTT, pre-installed and audio apps (tags)	DOOH
Device and browser characteristics	Make, model, device type, OS, version, screen, language, connection type, carrier name and network code, time-zone offset, as listed at tapmind.com/developers/privacy/data-collection	Browser type and version, OS, screen, language	Device type, OS, app version, as transmitted	None
Network and location	IP address (transient) and derived coarse location: country; region or city where permitted. Approximate device location under clause 4.2(c), from the SDK release that introduces it	IP address (transient) and derived coarse location: country; region or city where permitted		None
Consent and privacy signals	TCF, GPP, US Privacy, AddtlConsent, ATT status, limit-ad-tracking, age flags, mediation-platform privacy flags, publisher-set values	TCF/GPP strings as read from the page where the Services support it; opt-out flag	Consent, privacy and child flags as transmitted in tag parameters	None
Ad outcomes and diagnostics	Request, load, display, click, latency, error, revenue; crash and responsiveness counters (apps)			Aggregate plays
Inferences	Audience segments where personalised advertising is enabled and consented			None

Schedule 2 · Purposes and roles

ID	Purpose	Role	Identifier used	Publisher may exclude?
P1	Ad serving and demand-source selection, including improving the models that perform it	TapMind: Controller	Install identifier	No (core service)
P2	Reporting to the Publisher; TapMind's own reconciliation	TapMind: Processor (Publisher's reports); TapMind: Controller (own reconciliation)	Aggregated	No
P3	In-app frequency capping	TapMind: Controller	Install identifier (server-side counters)	No
P4	Sending ad requests to advertising partners	TapMind: Controller	Advertising identifier where permitted; approximate location where enabled	No (partners selectable per app)
P5	Cross-app frequency capping and reach (from the release that introduces it)	TapMind: Controller	Advertising identifier linked to install identifiers	Yes

ID	Purpose	Role	Identifier used	Publisher may exclude?
P6	Personalised advertising, audience segments (from the release that introduces it)	TapMind: Controller	Advertising identifier	Yes
P7	Attribution via advertisers' measurement partners	TapMind: Controller	Advertising identifier	Yes
P8	TapMind's own and direct advertisers' campaigns	TapMind: Controller	Per underlying purpose	Yes

Publisher exclusions for the Digital Properties under this Agreement: **[none | list of P-IDs]** (as recorded on the TapMind platform; exclusions take effect at the next configuration update of the Services).

Schedule 3 · Technical and organisational measures

- **Data minimisation**: the Services collect, and TapMind's tag parameters accept, only the data described in Schedule 1; the SDK's collected data and device storage are documented per release and disclosed publicly; user-provided data is discarded at ingress.
- **Published defaults and gated identifiers**: the SDK collects by default only what its public documentation states for that release; the advertising identifier and approximate location are enabled per Digital Property only after execution of this DPA and completion of the attestation, by an authorised TapMind administrator, with the action logged.
- **Consent handling**: Privacy Signals are read on each request where the Services support it, or received as transmitted by the Publisher's systems, forwarded unaltered, and checked before any disclosure to partners; withdrawal is applied on the next request; in the EEA, UK and Switzerland nothing is stored on the device without consent.
- **Encryption**: TLS 1.2 or higher in transit; encryption at rest for personal data; stored advertising identifiers additionally encrypted at the field level under managed keys.
- **Access control**: role-based access on a need-to-know basis; no routine human access to advertising identifiers; multi-factor authentication for administrative access.
- **Pseudonymisation**: serving logs are pseudonymised; erasure renders historical records unlinkable.
- **Logging and audit**: privileged actions logged with actor, time and reason and retained for audit.
- **Retention**: automated enforcement of the retention periods in Schedule 1 on every system that holds Service Data.
- **Vendor management**: written terms with sub-processors and advertising partners; partners unable to honour a Privacy Signal, or not registered under the applicable industry framework, are excluded from the request.
- **Hosting**: Infrastructure Providers at the locations listed at tapmind.com/legal/subprocessors; backups within the same region as the data they copy.
- **Incident response**: documented incident-response plan with defined notification paths; periodic exercise.
- **Personnel**: confidentiality obligations and privacy training for personnel with access to personal data.

Schedule 4 · Sub-processors and independent recipients

Category or entity	Role	Service	Location
Infrastructure Providers (cloud computing, hosting, storage, content delivery, networking, managed database, security, monitoring, messaging); the current providers and their data-processing terms are listed at tapmind.com/legal/subprocessors	Sub-processors	Infrastructure services	India (current); additional locations notified under clause 7.2
Website consent-management provider	Sub-processor (tapmind.com only)	Cookie consent on TapMind's own website	Per provider
Business-tooling providers (email, support, electronic signature, collaboration)	Sub-processors (business contact data only)	Operations	Various
Advertising partners enabled for the Digital Property	Independent controllers (recipients, not sub-processors)	Bidding on ad requests	Per partner; listed at tapmind.com/developers/privacy/partners
Attribution partners designated by advertisers	Independent recipients	Attribution (P7)	Per partner
Google LLC and affiliates	Independent recipient under the Publisher's own Google agreements	Ad serving via Google platforms	Global
TapMind Asia Pacific Pte. Ltd.	Contracting affiliate of the Controller; not a sub-processor of Service Data	Contracting	Singapore

Schedule 5 · Jurisdiction modules and country annexes

Module A (core): EEA, United Kingdom, Switzerland

A.1 Applicable law: GDPR, UK GDPR and Data Protection Act 2018, Swiss FADP, and national laws implementing the ePrivacy Directive.

A.2 **Transfers**: for Service Data transferred from the EEA to the Controller in India, the parties incorporate the Standard Contractual Clauses adopted by Commission Decision (EU) 2021/914 with the following selections: Module One (controller to controller) for Purposes where TapMind is Controller, and Module Two (controller to processor) for Purposes where TapMind is Processor; Clause 7 (docking) included; Clause 11 optional language not included; Clause 17 governing law: Ireland; Clause 18 forum: courts of Ireland; Annex I completed by Schedule 1 and the parties to this DPA, with TapMind Technologies Private Limited as data importer; Annex II by Schedule 3; Annex III by Schedule 4. For UK transfers, the International Data Transfer Addendum to the EU SCCs issued by the ICO is incorporated with the same selections. For Swiss transfers, the SCCs apply with the amendments recommended by the FDPIC. The Controller has carried out a transfer impact assessment, available to the Publisher on request.

A.3 **ePrivacy and the TCF**: the Publisher shall obtain End Users' consent for the storage of, and access to, information on the device or browser by the Services, including local storage on websites and the identifiers stored or read by the TapMind SDK in apps, through a consent management platform that supports the IAB Transparency and Consent Framework and includes TapMind as a vendor once TapMind's registration is complete; TapMind has applied to join the Framework and will publish its vendor ID at tapmind.com/privacy; until the registration is complete, the Controller serves only contextual advertising, stores nothing on the device and Processes no advertising identifier for EEA, UK or Swiss End Users. Once registered, the Controller Processes under the purposes and legal bases declared in its Global Vendor List entry (storing and accessing information on the device: consent; selecting advertising using limited data, measuring advertising performance, understanding audiences and developing services: legitimate interest or consent as the consent management platform signals; creating and using profiles for personalised advertising: consent), and the items it stores are disclosed at tapmind.com/legal/storage-disclosure.json.

A.4 **Representatives**: the Controller's representatives in the EU and the UK are being appointed and will be named at tapmind.com/privacy; until then, notices for the Controller may be sent to privacy@tapmind.com.

A.5 **Digital Services Act**: where the Digital Property is an online platform, the Publisher shall declare this on the platform and the parties shall exchange advertising transparency information through the IAB DSA transparency signals; the Publisher remains responsible for its Article 26 obligations.

Module B (core): India

B.1 Applicable law: Digital Personal Data Protection Act, 2023 and Rules thereunder.

B.2 **Roles**: the Controller, TapMind Technologies Private Limited, is the Data Fiduciary for the Purposes where it is Controller, whichever TapMind company has signed the Agreement.

B.3 **Notice and consent**: the Publisher shall ensure each Indian End User receives a notice meeting the Act's and Rules' requirements, itemising the Purposes, the Controller's identity, the means of withdrawal,

the grievance channel and the right to complain to the Data Protection Board, and shall obtain free, specific, informed, unconditional and unambiguous consent by clear affirmative action, passed to TapMind through the Services' consent interface or a consent management platform, or shall allow TapMind to present its own notice or to accept consent through a registered Consent Manager where the Services provide for it. Without a consent signal the Controller serves only contextual advertising. Consent may be withdrawn as easily as it was given.

B.4 **Children**: the Publisher shall declare apps directed at or used by children (under 18); TapMind does not provide the Services to such apps and shall not track, behaviourally monitor or direct targeted advertising at children.

B.5 **Breach**: the Controller shall notify the Publisher without undue delay and cooperate with notifications to the Board and affected Data Principals within the timelines in the Rules.

B.6 **Rights and grievances**: Grievance Officer: Naveen Chennala, Director, privacy@tapmind.com; requests answered within the period prescribed (not exceeding 90 days).

B.7 **Transfers**: Service Data is processed in India; transfers outside India are made only to countries not restricted by the Central Government.

B.8 **Retention**: purpose-limited; consent records retained as evidence for up to five years.

Module C (core): Singapore

C.1 Applicable law: Personal Data Protection Act 2012.

C.2 The Publisher shall obtain consent or rely on deemed consent by notification or the legitimate interests exception as permitted, and shall notify End Users of the Purposes.

C.3 **Transfer Limitation**: the Controller is bound by this DPA to provide a standard of protection comparable to the PDPA for Personal Data transferred from Singapore.

C.4 **Breach**: the Controller supports the Publisher's assessment and notification to the PDPC within three calendar days where a breach is notifiable.

C.5 Data Protection Officer: Naveen Chennala, Director, privacy@tapmind.com.

Module E (core): United States

E.1 Applicable law: state comprehensive privacy laws (including California, Colorado, Connecticut, Virginia, Texas, Oregon, Maryland and others), the Children's Online Privacy Protection Act, and FTC Act section 5.

E.2 **Roles**: for P4 to P8 the Controller is a third party and independent controller, and the disclosure of Service Data to it may constitute a "sale" or "sharing"; the Publisher shall provide the required notice and opt-out mechanisms, including recognition of opt-out preference signals where required, and shall pass opt-out signals to TapMind through the IAB Global Privacy Platform or the Services' consent interface.

E.3 **Multi-State Privacy Agreement**: the Controller is, or has applied to become, a signatory to the IAB Multi-State Privacy Agreement as amended and restated (the "MSPA") as a Downstream Participant under the National Approach. Where the Publisher is also a signatory, the MSPA governs the parties' transactions

covered by it, and this Module supplements it. Where the Publisher is not a signatory, this Module and Applicable Data Protection Law govern. The Controller passes the Privacy Signals it receives to its downstream partners unmodified, transacts only with partners identified as signatories on the MSPA identification list or bound by equivalent terms, maintains the deletion-request process required by the MSPA, and makes the partners it transacts with public at tapmind.com/developers/privacy/partners.

E.4 **Opted-out consumers**: where an End User has opted out of the sale or sharing of Personal Data or of targeted advertising, the Controller acts as the Publisher's service provider or processor for that End User and limits its Processing to the activities the MSPA permits for opted-out consumers (frequency capping, measurement, fraud prevention and viewability); it does not Process the advertising identifier, does not build or use a profile, does not combine the Personal Data with Personal Data from other sources, and does not sell or share it; and it notifies the Publisher if it can no longer meet these obligations.

E.5 **Processor purposes**: for P2 the Controller acts as a service provider or processor and shall Process Personal Data only for the business purposes in Schedule 2, shall not sell or share it, retain, use or disclose it outside the direct business relationship or for any purpose other than the Services, or combine it with Personal Data from other sources except as permitted.

E.6 **Sensitive data and children**: no sensitive Personal Data is Processed; the approximate location the Controller Processes is reduced on the device so that it does not identify an End User's location within the radius that any applicable state law treats as precise geolocation; no sale, sharing or targeted advertising with respect to consumers the parties know to be under 16; the child flag is honoured.

E.7 **Opt-out timing**: opt-outs are honoured on the next request and within 15 days for stored data.

E.8 **Third parties**: the Controller's written terms with every partner that receives Personal Data under this Module require the partner to comply with Applicable Data Protection Law, to provide the same level of protection as this Module, to honour opt-outs passed to it, to notify the Controller if it can no longer do so, and to impose the same obligations on anyone to whom it discloses the Personal Data.

Module I (core): General (all other jurisdictions)

I.1 Each party shall comply with the data-protection law of the End User's country.

I.2 Where that law requires consent, the Publisher shall obtain it or allow TapMind to; where it restricts transfers, the Controller relies on contractual safeguards in this DPA and, where the law requires data to remain in-country, Processes no identifier-linked Service Data for those End Users.

I.3 Where the law provides no data-protection framework, the parties apply the app-platform policies and this DPA as the minimum standard.

Schedule 6 · Publisher obligations

1. **Privacy notice.** Include in each Digital Property's privacy policy the TapMind disclosure text (or equivalent): TapMind Technologies Private Limited as controller, the Purposes, the data described in Schedule 1 for that property type, the link to tapmind.com/privacy, and how End Users can exercise choices. Update within 30 days of any change TapMind notifies.
2. **Consent.** Where required: (a) in the EEA, UK and Switzerland, use a consent management platform supporting the IAB Transparency and Consent Framework, Google-certified where the Publisher uses Google

ad platforms, and include TapMind and every enabled advertising partner as vendors once registered; (b) in the United States, provide opt-out mechanisms and pass signals through the Global Privacy Platform or the Services' consent interfaces; (c) in India and other consent-based jurisdictions, present a compliant notice and obtain consent covering TapMind and the Purposes, pass the result through the Services' consent interfaces, or permit TapMind to present its own notice where the Services provide one; (d) never obstruct, override or alter End Users' Privacy Signals; (e) where the Services are integrated through advertising tags, configure the ad server or other system to populate TapMind's consent and Privacy Signal parameters on every request.

3. **Identifiers on tag-based properties.** Configure the ad server or other system to transmit to TapMind only resettable advertising identifiers with their type, and never serial numbers, MAC addresses, hardware identifiers, precise geolocation, or user-provided data; transmit identifiers only where End Users' choices and Applicable Data Protection Law permit.
4. **Attestation.** Complete the attestation on the TapMind platform truthfully for each Digital Property, confirm it in writing, and update it within 30 days of any change, including property type, child-directed status or audience, platform program enrolment, CMP changes, and online-platform status.
5. **Platform and store disclosures.** Update Google Play Data Safety, Apple privacy labels, and any equivalent platform disclosures to reflect the Services using TapMind's mapping before identifier features are enabled, and declare approximate location as collected and shared for advertising before approximate device location is enabled for a Digital Property.
6. **Children.** Declare accurately; do not integrate the Services in mobile applications directed at children, including children in their declared audience, or enrolled in a child-focused platform program; set the device or app platform's child-directed and under-age flags where applicable.
7. **Inventory files.** Publish and maintain the ads.txt (websites) or app-ads.txt (apps, including CTV/OTT and audio apps) line TapMind issues for the Digital Property, and any sellers.json entries required by the TapMind Publisher Policies.
8. **Requests.** Forward End User requests concerning TapMind within five business days; use the platform's erasure mechanism where appropriate.
9. **Partners.** Enable only advertising partners whose disclosures the Publisher has included in its notice; TapMind provides the partner disclosure addendum.
10. **Services software.** Keep the SDK, adapters, tags and player within supported versions; do not modify them; do not extract or persist identifiers from them.