

TapMind Data Processing Addendum

Version 1.1, dated 9 October 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/v1.1 for reference only. In the event of any difference, the copy attached to the Agreement governs.

1. Definitions and precedence

- 1.1** "**TapMind Entity**" means the party to the Agreement, being either TapMind Asia Pacific Pte Ltd or TapMind Technologies Pvt Ltd, as identified in the Agreement. "**TapMind Group**" means both. "**Publisher**" means the other party to the Agreement. "**Personal Data**", "**Controller**", "**Processor**", "**Data Subject**", "**Processing**" and "**Supervisory Authority**" have the meanings given in Applicable Data Protection Law, and include their equivalents (such as "data fiduciary", "data principal", "organisation", "individual") 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 TapMind's software development kits, 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 the TapMind Group 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.
- 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 as Controller" in Schedule 2, the Publisher and the TapMind Entity 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 as Processor" in Schedule 2, the TapMind Entity 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 TapMind Entity 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 Intra-group. The Publisher acknowledges that the TapMind Entity may engage the other member of the TapMind Group as its Processor or, where the Publisher's users are in India and the Agreement is with TapMind Asia Pacific Pte Ltd, that TapMind Technologies Pvt Ltd may act as Processor in India, in each case under a written intra-group agreement imposing obligations no less protective than this DPA.

3. Publisher's obligations

3.1 The Publisher shall comply with Schedule 6, including:

- (a) providing End Users with a privacy notice that describes the categories of data the Services collect, the Purposes, the disclosure of data to advertising partners and the means to exercise rights; and, where Applicable Data Protection Law requires consent for identifier features, ensuring that TapMind is identifiable to End Users through the Publisher's consent management platform, a linked list of partners, or a statement in the notice that links to tapmind.com/privacy;
- (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;
- (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;
- (e) passing to TapMind, without alteration, the privacy signals set by End Users and by the device or app platform; and
- (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 or precise geolocation), and to transmit identifiers only where End Users' choices and Applicable Data Protection Law permit.

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.

4. TapMind's obligations

- 4.1** The TapMind Entity 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 TapMind Entity shall:
- (a) Process an End User's advertising identifier (or equivalent resettable device or browser identifier) only where the Publisher has enabled that feature for the Digital Property or transmits the identifier through the Services, Applicable Data Protection Law permits it, any required consent has been given and not withdrawn, the End User has not limited ad tracking or opted out, and the Digital Property is not directed at children;
 - (b) honour every privacy signal it receives within the time stated in Schedule 3;
 - (c) not collect precise geolocation, non-resettable device identifiers, contact information, or any data listed as "never collected" in Schedule 1;
 - (d) not create device fingerprints;
 - (e) not sell Personal Data for monetary consideration;
 - (f) apply the retention periods in Schedule 1;
 - (g) maintain the measures in Schedule 3; and
 - (h) 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 its SDKs.
- 4.3** The TapMind Entity 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; not to re-identify End Users, link identifiers to persistent identifiers, or fingerprint devices; to act on deletion requests forwarded by TapMind; and to comply with Applicable Data Protection Law. The TapMind Entity shall not disclose Service Data to any partner that cannot honour a privacy signal applicable to the request.

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 TapMind Entity accepts requests identified by install identifier or advertising identifier, 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 (applies to Schedule 2 "TapMind as Processor" Purposes only)

- 6.1** The TapMind Entity 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 TapMind Entity 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. The TapMind Entity shall impose on each sub-processor written obligations no less protective than this DPA and remains responsible for their performance.
- 7.2** The TapMind Entity 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; the TapMind Entity's measures are in Schedule 3.
- 8.2** The TapMind Entity 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 TapMind Entity 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 TapMind Group Processes Service Data in India. 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.

11. Retention and deletion

- 11.1** The TapMind Entity 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.

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 TapMind Entity 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, 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. The Publisher shall not use the Services in a mobile app that is directed at children, that includes children in its declared audience, or that is enrolled in a child-focused app-store program. On any other Digital Property directed at children, the TapMind Entity shall Process no advertising identifier and shall serve only contextual advertising. For any request from a mobile app that is flagged as relating to a child, the TapMind Entity shall serve no advertising; for such a request from any other Digital Property it shall Process no advertising identifier and shall serve only contextual advertising. The TapMind Entity 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 the TapMind Entity 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 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. The TapMind Entity 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 TapMind Entity 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: 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 (SDKs, 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 "Categories of Personal Data by property type" immediately below this schedule
Never collected	Name, contact details, account identifiers; precise geolocation; IMEI, serial, MAC, Android ID or other hardware or persistent device identifiers; any data that requires a runtime device permission; installed-app lists; device contents; biometric or special-category data; device or browser fingerprints; individual-level data from DOOH screens
Special categories	None; the TapMind Entity 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 and viewer identifiers up to 13 months from last seen; install identifier and profile up to 24 months from last activity; consent-choice records up to 5 years after withdrawal or erasure; pseudonymised serving logs up to 13 months; IP-bearing security logs up to 30 days). 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 for platform infrastructure and website hosting; Singapore for website-hosting backups; global for DNS and content-delivery edge locations). 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 without undue delay and within the periods required by Applicable Data Protection Law

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

Category	Mobile apps (SDK)	Websites (tag, video player)	CTV/OTT, pre-installed and audio apps (tags)	DOOH
Property and placement context	App ID, placement, format, partners, SDK version	Site, page context, placement, format	App bundle, channel or content context, placement, format	Screen and placement
Identifiers	Install identifier; session identifier; advertising identifier (GAID/IDFA) under clause 4.2(a)	Random viewer identifier and privacy-choice values held in browser local/session storage; no cookies	Resettable device advertising identifier and its type, as transmitted by the Publisher's ad server under clause 3.1(f)	None

Category	Mobile apps (SDK)	Websites (tag, video player)	CTV/OTT, pre-installed and audio apps (tags)	DOOH
Device and browser characteristics	Make, model, OS, version, screen, language, connection type, carrier name, time-zone offset	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			None
Consent and privacy signals	TCF, GPP, US Privacy, AddtlConsent, ATT status, lmt , age 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	Request, load, display, click, latency, error, revenue			Aggregate plays
Inferences	Audience segments where personalised advertising is enabled and consented			None

For mobile apps the device characteristics also include device type, mobile network code, pixel ratio and app version, and the property data includes the placement code and name. Where enabled for the Digital Property, the TapMind Entity also Processes: device state and capability in bucketed form (power, memory, storage, audio, display and network quality); app engagement counters in bucketed form; and integrity indicators, used for fraud prevention only. No identifier is derived from these values and they are not disclosed to Demand Partners.

Schedule 2 · Purposes and roles

ID	Purpose	Role	Identifier used	Publisher may exclude?
P1	Ad serving and demand-source selection	TapMind as Controller	Install identifier	No (core service)
P2	Reporting to the Publisher; TapMind's own reconciliation	TapMind as Processor (Publisher's reports); TapMind as Controller (own reconciliation)	Aggregated	No
P3	In-app frequency capping	TapMind as Controller	Install identifier	No
P4	Sending ad requests to advertising partners	TapMind as Controller	Advertising identifier where permitted	No (partners selectable per app)
P5	Cross-app frequency capping and reach	TapMind as Controller	Advertising identifier	Yes
P6	Personalised advertising, audience segments	TapMind as Controller	Advertising identifier	Yes
P7	Attribution via advertisers' measurement partners	TapMind as Controller	Advertising identifier	Yes
P8	TapMind's own and direct advertisers' campaigns	TapMind as 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 within 60 seconds of recording).

Schedule 3 · Technical and organisational measures

- **Data minimisation:** the Services collect, and TapMind's tag parameters accept, only the data described in Schedule 1; for the SDKs, collected data is documented per release.
- **Default-off:** where the Services provide identifier-related features (the SDKs), they operate on a Digital Property only after enablement on the platform following execution of this DPA and completion of the attestation; enablement is 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.
- **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.
- **Vendor management:** written terms with sub-processors and advertising partners; partners unable to honour a privacy signal 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

Entity	Role	Service	Location
Infrastructure Providers (cloud, hosting, storage, content delivery, networking, managed database, security, monitoring, messaging), currently Akamai Technologies Solutions (India) Private Limited (Akamai Cloud), Amazon Web Services, Amazon Route 53, BlazingCDN and Hostinger; full list with locations at tapmind.com/legal/subprocessors	Sub-processors	Infrastructure services	India (platform infrastructure and website hosting); Singapore (website-hosting backups); global (DNS and content-delivery edge locations); additional locations notified under clause 7.2
TapMind Technologies Pvt Ltd (where the TapMind Entity is TapMind Asia Pacific Pte Ltd)	Sub-processor / intra-group Processor	Platform operation and hosting	India
Advertising partners enabled for the Digital Property	Independent Controllers (recipients, not sub-processors)	Bidding on ad requests	Per partner; listed on the platform per Digital Property
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

Current list: tapmind.com/legal/subprocessors .

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 TapMind Entity or the TapMind Group 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 this DPA's parties; 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 (references to the GDPR read as references to the FADP; the FDPIC as competent authority; Swiss law for Swiss data subjects' claims). The TapMind Group has carried out a transfer impact assessment, available to the Publisher on request.
- A.3** **ePrivacy:** the Publisher shall obtain End Users' consent for the storage of, and access to, information on the device or browser by the Services (including cookies, local storage and similar technologies on websites and identifiers read by the SDKs in apps) except where strictly necessary, through a consent management platform that supports the IAB Transparency & Consent Framework and includes TapMind (vendor ID to be listed at tapmind.com/privacy once issued) once TapMind is registered; until then, the TapMind Entity Processes no advertising identifier for EEA, UK or Swiss End Users.
- A.4** **Representatives:** the TapMind Entity shall appoint, and notify to the Publisher, representatives in the EU and the UK before any Processing of EEA or UK End Users' Personal Data under this DPA.
- 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 TapMind Entity is a Data Fiduciary for the Purposes where it is Controller; where the TapMind Entity is TapMind Asia Pacific Pte Ltd, it is a Data Fiduciary for Indian Data Principals and TapMind Technologies Pvt Ltd acts as its Data Processor under a written contract as required by the Act.
- 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, TapMind'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, or shall allow TapMind to

present its own notice or to accept consent through a registered Consent Manager. Consent may be withdrawn as easily as it was given.

- B.4 Children:** the Publisher shall declare apps used by children (under 18) and the TapMind Entity shall not track, behaviourally monitor or direct targeted advertising at children, nor Process a child's personal data without verifiable parental consent where the Act requires it.
- B.5 Breach:** the TapMind Entity 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.

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 TapMind Entity ensures that recipients outside Singapore, including TapMind Technologies Pvt Ltd, are bound by legally enforceable obligations to provide a standard of protection comparable to the PDPA, through the intra-group agreement and this DPA.
- C.4 Breach:** the TapMind Entity supports the Publisher's assessment and notification to the PDPC within three calendar days where a breach is notifiable.
- C.5** DPO: 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 §5.
- E.2 Roles:** for P4 to P8 the TapMind Entity is a third party/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 GPP framework or the SDK consent interface.
- E.3** For P2 (Processor), the TapMind Entity acts as a "service provider"/"processor": it 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, and shall notify the Publisher if it can no longer meet these obligations.

- E.4 Sensitive data and children:** no sensitive Personal Data is Processed; no sale, sharing or targeted advertising with respect to consumers the parties know to be under 16; `regs . coppa` honoured.
- E.5 Opt-out timing:** opt-outs are honoured on the next request and within 15 days for stored 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 TapMind Entity 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.** Describe in each Digital Property's privacy policy the data listed in Schedule 1 for that property type, the Purposes, the disclosure of data to advertising partners, and how End Users can exercise their choices. Where Applicable Data Protection Law requires consent for identifier features, make TapMind identifiable to End Users: in the consent management platform's vendor list, in a linked list of partners, or in a statement that links to tapmind.com/privacy . Update within 30 days of any change TapMind notifies.
2. **Consent.** Where required: (a) in the EEA, UK, Switzerland and Canada, use a consent management platform supporting the IAB TCF (Canada policy where applicable), Google-certified where the Publisher uses Google ad platforms, and include TapMind and every enabled advertising partner as vendors; (b) in the United States, provide opt-out mechanisms and pass signals through GPP 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, or pass the Publisher's own notice 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, 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 the Services are used in the Digital Property. Declare every data type in the mapping as collected and shared.
6. **Children.** Declare accurately; do not use the Services in a mobile app that is directed at children or that includes children in its declared audience; do not enable identifier features on any child-directed Digital Property; set the device or app platform's child-directed and under-age flags where applicable.
7. **Inventory files.** Maintain accurate ads.txt (websites), app-ads.txt (apps, including CTV/OTT and audio apps) and sellers.json entries for TapMind and its partners as 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 SDKs, tags and player within supported versions; do not modify them; do not extract or persist identifiers from them.