Advertising Privacy Policy

1. Who we are and scope

1.1. This Internet Advertising Privacy Policy (the "**Policy**") describes how TrueData Audiences LLC, a Delaware limited liability company, with its registered office at 251 Little Falls Drive, Wilmington, DE 19808, United States, registered with the Secretary of State of the State of Delaware under file number 10782954 ("**Company**", "**we**", "**us**" or "**our**") processes data in connection with data analytics, audience creation, identifier matching, advertising delivery, retargeting, measurement and related online advertising services (the "**Services**").

1.2. This Policy applies to pseudonymous data relating to browsers, devices, advertising identifiers and online activity used in the Services ("**Service Data**"). It does not apply to ordinary website use, business contacts, recruitment or investor communications, which are covered by our separate Privacy Policy.

1.3. For the Services, the Company acts as an independent controller where it determines the purposes and essential means of processing.

1.4. You can contact us regarding privacy matters at dataprivacy@truedata.co or by post at our registered office address stated above.

2. How the Services work

2.1. We receive or collect Service Data from our own technologies, client integrations, publishers, website and app operators, advertising exchanges, advertising-technology platforms, data partners and other participants in the digital advertising ecosystem (together, "**Partners**"). The exact sources depend on the relevant Service and market.

2.2. We use Service Data to create or maintain pseudonymous profiles and audience segments, for example groups of identifiers likely to be interested in a product category. We may make segment lists, identifier lists, matching signals or aggregated insights available to clients and advertising-technology platforms so that they can select, deliver, limit, measure or analyze advertising.

2.3. We contractually require Partners that provide or enable collection of Service Data to give users legally required information, obtain and pass valid consent or other required legal signals, respect opt-outs and deletion requests, and provide Service Data lawfully.

2.4. We generally do not have a direct relationship with individual users whose identifiers are included in Service Data. For this reason, our ability to respond to individual requests depends on receiving the relevant identifier, as explained in Section 9.

3. Service Data we process

3.1. Depending on the Service and the source, Service Data may include:

- online and device identifiers, such as cookie IDs, mobile advertising IDs (for example IDFA or Google Advertising ID), connected-TV identifiers and internal pseudonymous identifiers;
- hashed identifiers, such as hashed email addresses or hashed telephone numbers, where supplied in hashed form for matching. We do not use such values to identify individuals by name and we do not reverse them;
- technical data and bid-request data, such as IP address, user agent, device type, browser type, operating system, language, timestamp, advertising placement and auction information;
- approximate location, such as country, region, city or location inferred from IP address or supplied in generalized form. We do not use precise GPS location for the Services;
- online activity and interest signals, such as website or app categories, app usage, page or content categories, ad interactions and purchase-intent signals;
- demographic or household-level attributes where supplied by Partners or inferred in ranges, such as age band, likely gender, language, general income tier or broad geographic region;
- derived segments and inferences, such as interest categories, audience memberships, model scores or aggregated audience insights;
- consent, opt-out, deletion, suppression and compliance records needed to honour choices and demonstrate compliance.

3.2. We do not collect names, postal addresses, plain-text email addresses, plain-text telephone numbers, government identification numbers or payment card details for the Services. We do not seek to identify users by name, and we contractually prohibit recipients from using Service Data to identify, contact or make decisions about an individual outside the permitted advertising purposes.

3.3. We do not create, use or sell audience segments designed to reveal special-category or sensitive characteristics, such as racial or ethnic origin, political opinions, religion, trade-union membership, genetic or biometric data, health, sex life, sexual orientation, precise location, or children's data. If we become aware that such data has been received contrary to our requirements, we take steps to delete or exclude it.

4. Technologies used

4.1. On properties operated by Partners or clients, the Services may involve cookies, pixels, tags, server-to-server integrations, software development kits, identity matching tools and similar technologies. These technologies may store information on, or access information from, a browser or device, synchronize identifiers between systems, and link identifiers that appear to relate to the same browser, device or household. Such activities are performed only where the required consent or other legal basis has been obtained or passed to us.

5. Purposes and legal bases

5.1. We process Service Data for the following purposes:

- Audience creation and enrichment: building, maintaining, updating and validating pseudonymous profiles, segments, scores and inferences.
- Advertising delivery and retargeting: helping clients select, deliver, cap, sequence and personalize advertising based on Service Data.
- Identifier matching and activation: matching identifiers across systems, platforms, devices and channels to activate or suppress audiences.
- Measurement and analytics: measuring reach, frequency, campaign performance, conversions, audience composition and aggregated insights.
- Product improvement: testing, quality control, modelling, deduplication, data accuracy, data minimization and service development.
- Security and fraud prevention: detecting invalid traffic, abuse, bot activity, security incidents and unauthorized access.
- Compliance and legal claims: honoring consents, opt-outs and deletion requests, maintaining suppression lists, responding to lawful requests and defending legal claims.

5.2. Where the GDPR, UK GDPR or equivalent EEA rules apply, our legal bases are:

- consent - for storing or accessing information on a device and for personalized advertising activities where consent is required by e-privacy rules, the GDPR / UK GDPR, TCF policies or applicable guidance;
- legitimate interests - for security, fraud prevention, technical delivery, aggregate measurement, product improvement, compliance records and legal claims, in each case only where permitted and subject to balancing and the right to object;
- legal obligation - where processing is necessary to comply with binding legal or regulatory obligations.

5.3. In Canada, we rely on meaningful consent obtained by us or by Partners, and on statutory exceptions where applicable. In the United States, use or disclosure of Service Data for targeted advertising may be considered a "sale", "sharing" or "targeted advertising" under some state privacy laws, even where no money is exchanged. Your choices are described in Sections 9 and 10.

5.4. The Services involve profiling in the sense of assigning pseudonymous identifiers to advertising segments. This profiling is used for advertising and analytics.

6. Recipients

6.1. We may disclose Service Data, or make it available, to the following categories of recipients:

- clients, such as advertisers, brands, agencies, publishers and media owners;

- advertising-technology platforms, such as DSPs, SSPs, DMPs, CDPs, ad exchanges, ad networks, clean rooms, onboarding providers, identity providers and measurement providers;
- data and analytics vendors that help us classify, validate, model, enhance or measure Service Data, subject to contractual restrictions;
- infrastructure and security providers, such as cloud, hosting, storage, connectivity, monitoring and IT-security providers acting as processors or service providers;
- professional advisers, auditors, insurers and transaction counterparties under confidentiality arrangements;
- courts, regulators and public authorities where disclosure is required by law or a valid and binding request, after assessing legality and scope.

6.2. Recipients that receive Service Data as independent controllers are responsible for their own use, privacy notices and compliance. We contractually restrict recipients from re-identifying users, using Service Data for prohibited sensitive purposes, or retaining Service Data beyond the agreed purposes.

7. International transfers

7.1. The Services are international.

7.2. Where EEA personal data is transferred outside the EEA, we rely on adequacy decisions where available, including the United Kingdom, Canada for commercial organizations subject to PIPEDA, and the EU-US Data Privacy Framework for certified US recipients. Where no adequacy decision applies, we use Standard Contractual Clauses adopted by the European Commission, supplemented where necessary by transfer impact assessments and additional safeguards. For UK personal data, we use UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, as applicable.

7.3. Information about relevant safeguards, including a copy of applicable contractual clauses redacted for commercial and confidential information, is available on request.

8. Retention

8.1. We retain Service Data for no longer than necessary for the relevant Service and legal obligations. Unless a shorter period applies, pseudonymous Service Data used for audience creation and advertising activation is retained for a maximum of 12 months from the last activity associated with the relevant identifier. We may retain suppression records, opt-out records, deletion logs and compliance records for longer where necessary to honor choices, evidence compliance, prevent re-collection or defend legal claims.

8.2. Service Data is deleted, de-identified or excluded from active use when: (a) the retention period expires; (b) we execute a valid deletion or opt-out request; (c) we receive a valid withdrawal, deletion or suppression signal from a Partner; (d) the relevant advertising identifier is reset or deleted and the signal reaches our systems; or (e) we determine that the data was obtained contrary to our requirements.

9. Your rights and choices

9.1. Subject to applicable law, you may have the right to access, know, obtain a copy, correct, delete, restrict or object to processing of Service Data, withdraw consent, opt out of sale, sharing or targeted advertising, and lodge a complaint with a competent authority.

9.2. You may exercise your choices by contacting us at dataprivacy@truedata.co and providing the information reasonably necessary for us to identify the relevant browser, device or advertising identifier. You may also use the privacy, consent, cookie or advertising settings available in your browser, device, website or application, where applicable. Where required by applicable law and technically supported by the relevant Service, we will also respect recognized opt-out preference signals.

9.3. We will respond to requests within the time limits required by applicable law. We may deny or limit a request where we cannot match the request to an identifier, where the request is not verifiable, where an exemption applies, or where complying would adversely affect the rights and freedoms of others.

10. Jurisdiction-specific information

10.1. EEA, United Kingdom. The GDPR / UK GDPR applies together with local data-protection and e-privacy rules. For advertising technologies that store or access information on a device, consent is required unless an exemption applies. You may complain to the supervisory authority competent for your habitual residence, place of work or the place of the alleged infringement.

10.2. Canada. Where PIPEDA or substantially similar provincial laws apply, we and/or our Partners obtain meaningful consent appropriate to the sensitivity of the data and reasonable expectations of the individual. You may withdraw consent using the tools described above, subject to legal or contractual restrictions and reasonable notice.

10.3. United States. Where a US state comprehensive privacy law applies to us and to you, you may have rights to know, access, correct, delete and obtain a copy of personal information, and to opt out of sale, sharing, targeted advertising and certain profiling. Use or disclosure of Service Data for targeted advertising may be considered a sale or sharing under some laws. You may exercise opt-out rights through the tools in Section 9.

10.4. Requests may be denied where the requester cannot be matched to an identifier in our systems, the request is not verifiable, or a legal exemption applies.

11. Children

11.1. The Services are not directed to children. We contractually require Partners not to provide data from websites, apps or services directed to children and not to provide data relating to users known to be under 16. If we become aware that such data has been received, we delete or exclude it.

12. Security

12.1. We apply appropriate technical and organizational measures designed to protect Service Data, including pseudonymization by design, hashing or tokenization where appropriate, encryption in transit, access controls, logging, environment segregation, retention controls, partner and processor contractual safeguards, and incident-response procedures.

13. Changes to this Policy

13.1. We may update this Policy to reflect changes in law, industry frameworks, technologies, Partners or our Services. This Policy is for information purposes and does not create contractual rights beyond those provided by applicable law.