Privacy Policy

1. Who we are and scope of this Policy

1.1. This Privacy Policy (the "**Policy**") explains 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**") collects, uses and protects personal data when you use our website at https://www.truedata.co/ (the "**Website**"), contact us, communicate with us in a business context, subscribe to communications, attend our events, apply for a role, or otherwise interact with us outside our advertising services.

1.2. The Company is the controller of the personal data described in this Policy. In Canada, the Company is the organization accountable for personal information processed under this Policy.

1.3. This Policy does not apply to: (a) processing performed by third-party websites, platforms or services linked from the Website; or (b) processing connected with our data analytics and online advertising services, including audience segments, identifier matching and advertising measurement. That processing is described in our separate Internet Advertising Privacy Policy.

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

2. Personal data we collect

2.1. We collect only the data reasonably necessary for the purposes described below. This may include:

- contact and business identification data, such as name, business email address, telephone number, employer or principal, job title and business address;
- correspondence data, including the content of messages, enquiries, requests, meeting notes and attachments that you choose to provide;
- contract and transaction data, such as information needed to negotiate, conclude or perform a contract with a client, supplier or partner;
- newsletter and event data, such as email address, communication preferences, consent records, attendance records and event participation information;
- recruitment data, such as CV, cover letter, employment history, qualifications, interview notes and any information you provide in the recruitment process;
- technical and usage data, such as IP address, device and browser type, operating system, language, referring URL, pages viewed, access times and approximate location derived from IP address;
- cookie and similar technology data, where used on the Website, as described in Section 8 and in the cookie banner or consent tool.

2.2. We may receive business contact data directly from you, from your employer or principal, from publicly available business sources (such as company registers, professional networks and corporate websites), or from business partners where there is a legitimate reason to contact you.

2.3. Providing personal data is usually voluntary, but some data may be necessary to respond to your enquiry, communicate with you, conclude or perform a contract, comply with law, or run a recruitment process.

3. Purposes and legal bases

3.1. Where the GDPR, UK GDPR or equivalent EEA rules apply, we rely on the legal bases listed below. In Canada, we rely on express or implied consent where required, and on permitted exceptions under PIPEDA or applicable provincial law. In other jurisdictions, we rely on the corresponding lawful bases available under applicable law.

3.2. We process personal data for the following purposes and on the following legal bases:

- to operate, secure and improve the Website, prevent fraud, abuse and security incidents, and produce aggregated statistics. For this purpose, we process technical and usage data and

strictly necessary cookies. We rely on our legitimate interests in operating a secure and functional website, and on legal obligations where applicable;

- to respond to enquiries and business communications, conduct pre-contractual contacts, and negotiate, conclude and perform contracts. For this purpose, we process contact data, business identification data, correspondence data and contract data. We rely on the performance of a contract or steps taken before entering into a contract, and on our legitimate interests where you act on behalf of an organization;

- to manage relationships with clients, suppliers, partners, investors and to carry out internal administration and reporting. For this purpose, we process contact data, business identification data, correspondence data and contract data. We rely on our legitimate interests in managing business relationships;

- to send newsletters, event invitations and marketing communications about our own products and services. For this purpose, we process contact data, communication preferences, consent records and unsubscribe records. We rely on consent where required by e-privacy or anti-spam laws, and otherwise on our legitimate interests;

- to conduct recruitment and assess candidates. For this purpose, we process recruitment data. We rely on steps taken before entering into a contract, legal obligations, and consent where required for future recruitment or optional data;

- to comply with accounting, tax, corporate, regulatory and record-keeping obligations, and to respond to lawful requests from public authorities. For this purpose, we process all relevant categories of personal data, as necessary. We rely on legal obligations and, where applicable, our legitimate interests in documenting compliance;

- to establish, exercise or defend legal claims, conduct audits, manage risk and carry out corporate transactions. For this purpose, we process all relevant categories of personal data, as necessary. We rely on our legitimate interests in protecting our legal position and conducting corporate transactions.

3.3. Where we rely on legitimate interests, we assess whether the processing is necessary and proportionate and whether your interests, rights and freedoms override our interests. You may object to such processing as described in Section 7.

3.4. We do not use data covered by this Policy for decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you.

4. Recipients

4.1. We disclose personal data only where necessary, proportionate and subject to appropriate safeguards. Recipients may include:

- service providers, such as hosting, cloud, IT support, CRM, email delivery, analytics, cookie consent, security, document management and recruitment tools;
- professional advisers, auditors, insurers, banks and other parties bound by confidentiality;
- courts, public authorities, regulators and law-enforcement bodies, where disclosure is required by law or a valid and binding request. We assess the legal basis and scope of such requests and disclose no more than reasonably required;
- prospective or actual buyers, sellers, investors, lenders and their advisers in connection with a merger, acquisition, financing, restructuring or other corporate transaction, subject to confidentiality and appropriate safeguards.

4.2. We do not sell personal data covered by this Policy. Choices relating to audience data, targeted advertising, sale/sharing and similar concepts under US state privacy laws are described in the Internet Advertising Privacy Policy.

5. International transfers

5.1. We operate internationally and may transfer personal data between the jurisdictions.

5.2. Where EEA personal data is transferred outside the EEA, we rely on an adequacy decision where available, including adequacy decisions for 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.

6. Retention

6.1. We keep personal data only for as long as necessary for the purposes for which it was collected, and then for as long as required or permitted by law. We determine retention by reference to the duration of the relationship or correspondence, statutory retention duties, limitation periods and the need to evidence compliance.

- enquiries not leading to a contract: usually up to 12 months from the last meaningful contact;
- contract and business relationship data: for the duration of the relationship and thereafter for limitation periods and statutory retention obligations;
- marketing communication data: until you unsubscribe, withdraw consent or object, plus a limited period needed to evidence compliance;
- website technical logs: usually up to 12 months unless longer retention is needed for security or legal claims;
- recruitment data: for the duration of the process and, where permitted or consented to, up to 12 months for future recruitment.

6.2. After the applicable retention period, data is deleted, anonymized or securely archived where retention is required by law or legal claims.

7. Your rights

7.1 Subject to the conditions and limitations of applicable law, you may have the right to access your personal data, receive a copy, rectify inaccurate or incomplete data, erase data, restrict processing, object to processing based on legitimate interests, object to direct marketing, receive data portability, withdraw consent at any time, and lodge a complaint with a supervisory authority.

7.2. To exercise your rights, contact us using the details in Section 1.4. We may need to verify your identity in a proportionate manner. We will respond within the statutory time limit. In the EEA and UK this is generally one month, extendable where permitted by law. In Canada and applicable US states, we respond within the periods required by applicable law.

7.3. You may complain to the authority competent for your place of residence, place of work or the place of the alleged infringement. We would appreciate the opportunity to address your concerns first.

8. Cookies and similar technologies

8.1. The Website may use cookies, pixels, local storage and similar technologies. Strictly necessary technologies are used to provide the Website and maintain security. Non-essential technologies, such as analytics, functional or marketing cookies, are used only where permitted by law and, where required, after your consent through the cookie banner or consent tool.

8.2. You may change or withdraw consent at any time through the "Cookie settings" link on the Website or through your browser settings. Withdrawing consent does not affect prior lawful processing and may affect Website functionality.

9. Security

9.1. We use appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. Measures may include access controls, encryption in transit, logging, need-to-know access, processor due diligence, contractual safeguards, backups and incident-response procedures.

10. Children

10.1. The Website and our ordinary business services are directed at business users and adults. We do not knowingly collect personal data from children under 16. If you believe a child has provided us with personal data, please contact us and we will take appropriate steps to delete it.

11. Jurisdiction-specific information

11.1. Canada. Where PIPEDA or substantially similar provincial laws apply, we collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances, with consent where required and subject to permitted exceptions. You may withdraw consent subject to legal or contractual restrictions and reasonable notice. For Quebec residents, additional rights may apply, including rights relating to access, correction, de-indexation / cessation of dissemination where statutory conditions are met, and information about profiling technologies and means to activate or deactivate them. Commercial electronic messages are sent in compliance with Canada's Anti-Spam Legislation, including consent and unsubscribe requirements.

11.2. 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 certain processing such as targeted advertising, sale or sharing. The ordinary website and business-contact data covered by this Policy is not sold or shared for cross-context behavioural advertising by us. Choices relating to our advertising services are described in the Internet Advertising Privacy Policy. We do not discriminate against you for exercising privacy rights and we honour opt-out preference signals where required by law.

11.3. EEA, United Kingdom. The GDPR / UK GDPR applies together with local implementing and e-privacy rules.

11.4. Nothing in this Policy limits rights granted by above mentioned laws.

12. Changes to this Policy

12.1. We may update this Policy to reflect changes in law, technology, industry practice or our operations. The current version, including its effective date, is available on the Website. This Policy is for information purposes and does not create contractual rights beyond those provided by applicable law.