Introduction

Tag Digital ("we," "us," "our") is committed to protecting your privacy. This Privacy Policy outlines how we collect, use, and safeguard your personal data ensuring compliance with relevant laws including but not limited to GDPR + CCPA.

1. Definitions

1. **Customer Personal Data:** Personal data within the Customer Database provided to Supplier by or on behalf of Customer or within the Subscriber Database.
2. **Controller's Personal Data:** The Customer Personal Data and/or the Supplier Personal Data, as applicable.
3. **Data Protection Legislation:** All relevant laws protecting individual privacy rights, including GDPR, CCPA, and various state laws in the US.
4. **GDPR:** Regulation (EU) 2016/679 on the protection of natural persons regarding personal data processing.
5. **Data Subject:** A living individual who is the subject of personal data.
6. **Information Security Incident:** A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
7. **Security Documentation:** All documents and information made available for security reviews.
8. **Supplier Personal Data:** Personal data within the Subscriber Database provided to Customer by Supplier.
9. **Subprocessors:** Third parties authorized to process personal data on behalf of Supplier.

2. Data Ownership

- **Customer Owns:** Customer Personal Data. Tag Digital processes this data on behalf of the Customer and must comply with the Customer's instructions and applicable data protection laws.
- **Tag Digital Owns:** Supplier Personal Data. The Customer may process this data under the terms agreed upon but must comply with Tag Digital's instructions and applicable data protection laws.

3. Duration of Policy

This Policy is effective from the Effective Date of the Agreement and remains in force until the deletion of all personal data by both parties.

4. Data Processing

4.1 **Roles and Compliance:**

- Supplier acts as a processor for Customer Personal Data.
- Customer acts as a controller for Customer Personal Data.

- Compliance with applicable Data Protection Legislation is mandatory.

4.2 **Scope of Processing:**

- Process data only as per documented instructions from the controller.
- Prohibit selling, sharing, or using data for unauthorized commercial purposes.

5. Data Deletion

Upon termination, delete or return all personal data and provide written certification within 60 days unless retention is required by law.

6. Data Security

6.1 **Security Measures:**

- Implement and maintain appropriate security measures in line with industry standards.
- Ensure all personnel who have access to personal data are obliged to keep the data confidential.

6.2 **Information Security Incidents:**

- Notify the controller without undue delay in the event of a data breach.
- Take steps to mitigate and prevent future incidents.

6.3 **Controller's Responsibilities:**

- Controller is responsible for reviewing security measures and backing up personal data.
- Controller must ensure all necessary consents and notices are in place for lawful data transfer.

6.4 **Reviews and Audits:**

- Allow audits at least once per year
- Provide all necessary information for audits and ensure compliance with data protection requirements.

7. Impact Assessments and Consultations

Assist the controller with data protection impact assessments and consultations as required by law.

8. Data Subject Rights

8.1 **Responsibility for Requests:**

- Notify the controller of any data subject requests.

8.2 **Assistance with Requests:**

- Provide reasonable assistance to the controller in responding to data subject requests.

9. Data Transfers

Store and process data only as per the documented instructions of the controller. Any transfer outside the EEA requires prior written consent and appropriate safeguards.

10. Subprocessors

10.1 **Consent:**

- Obtain consent for any subprocessor engagement.
- Enter into written contracts with subprocessors, ensuring data protection obligations are met.

10.2 **Information:**

- Provide information about subprocessors and allow objections.

11. Processing Records

Maintain records of processing activities as required by GDPR.

12. Liability

Total combined liability of Processor, including subprocessors, is as per the Agreement. This includes limits on liability for certain types of loss such as loss of profits, sales, business, agreements, anticipated savings, software, data, information, goodwill, and indirect or consequential loss.

13. Effect of Terms

In case of any conflict, the terms of this policy prevail over other agreements.

Contact Us

For any questions or requests regarding your personal data, please contact us craig@tagdigital.co.uk

This policy ensures compliance with GDPR, CCPA, and other relevant legislation, providing transparency and protection for personal data. For further details, please refer to the complete terms.