CHAPTER 42. SAN MANUEL PRIVACY ACT[1]

SMTC 42.1 Short Title

This Chapter shall be known and cited as the "San Manuel Privacy Act" (hereinafter the "Act").

SMTC 42.2 Findings

42.2.1 The San Manuel Band of Mission Indians (the "Tribe") is a sovereign, federally-recognized Indian tribe with inherent jurisdiction over the lands of the San Manuel Indian Reservation and other lands held in trust by the United States for the benefit of the Tribe (collectively, "Tribal Trust Lands").

42.2.2 The Tribe makes the following findings with respect to individual privacy and the processing of personal data collected from persons located on Tribal Trust Lands:

(a) The Tribe respects privacy as an element of individual freedom and values individual personal privacy.

(b) The Tribe and its affiliates routinely collect personal data for governmental and business purposes.

(c) The Tribe desires to provide individuals with a process to understand what type of personal data has been collected on Tribal Trust Lands and an opportunity to opt-out of any potential sale of their information.

(d) There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. This growth has the potential for great benefits to human knowledge, technological innovation, and economic growth, but also the potential to impact individual privacy and freedom.

42.2.3 The Tribe desires to ensure that the principles of transparency, choice, and control are reflected in the rights provided to individuals on Tribal Trust Lands from whom personal data is collected.

SMTC 42.3 Purposes

42.3.1 This Act is adopted by the Tribe, acting through its General Council in the exercise of its inherent sovereign power to enact ordinances and otherwise safeguard and provide for the health and welfare of the Tribe, its Citizens, and other persons located on Tribal Trust Lands.

42.3.2 The purpose of this Act is to establish the roles and responsibilities of the Tribe and its affiliates as controllers and processors of consumer data collected on Tribal Trust Lands and the rights of consumers with respect to such collected data.

[1] Adopted by the General Council on November 12, 2019.

SMTC 42.4 Definitions

42.4.1 In this Act the following terms shall have the following meanings:

(a) **"Affiliate"** means a legal entity that controls, is controlled by, or is under common control with, another legal entity.

(b) **"Business purpose"** means the processing of personal data for or on behalf of the controller's operational purposes, or other notified purposes, provided that the processing of personal data is reasonably necessary to carry out those purposes. Business purposes include, but are not limited to:

i. Auditing related to a current interaction with the consumer and concurrent transactions including, but not limited to, counting advertisement impressions, verifying positioning and quality of advertisement impressions, and auditing compliance with this specification and other standards;

ii. Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity;

iii. Identifying and repairing errors that impair existing or intended functionality;

iv. Short-term, transient use, including, but not limited to, the contextual customization of advertisements shown as part of the same interaction;

v. Maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;

vi. Undertaking internal research for technological development;

vii. Authenticating a consumer's identity; or

viii. Protecting the health and welfare of the Tribe, its affiliates, and individuals on Tribal Trust Lands.

(c) **"Consent"** means a clear affirmative act signifying a specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

(d) **"Consumer"** means a natural person whose personal data is collected by the San Manuel Band of Mission Indians or its affiliates on Tribal Trust Lands. It does not include data collected from a natural person acting in a commercial or employment context.

(e) **"Controller"** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Tribe or its affiliate(s) may be deemed a "controller" or "processor" (as defined below) as applicable.

(f) **"Deidentified data"** means:

i. Data that cannot be reasonably linked to a known natural person without additional information kept separately; or

ii. Data (1) that has been modified to a degree that the risk of reidentification is small, and (2) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls.

(g) **"Identified or identifiable natural person"** means a person who can be readily identified.

(h) **"Personal data"** means any information that is linked or reasonably linkable to an identified or identifiable natural person. Personal data does not include deidentified data or publicly available information. For these purposes, "publicly available information" means information that is lawfully made available from federal, state, local, or tribal government records.

(i) **"Process"** or **"processing"** means any collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(j) **"Processor"** means a natural or legal person that processes personal data on behalf of the controller.

(k) **"Restriction of processing"** means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

(l) **"Sale," "sell,"** or **"sold"** means the provision of personal data by the controller to a third party in exchange for monetary consideration and for an intended use outside of the controller's business purpose.

"Sale" does not include the following: (i) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets.

(m) **"Targeted advertising"** means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from tracking a consumer's activities across nonaffiliated web sites, applications, or online services to predict user preferences or interests.

(n) **"Third party"** means a natural or legal person other than the consumer, controller, processor, or an affiliate or processor of the processor or of the controller.

(o) **"Tribe"** or **"Tribal"** means the San Manuel Band of Mission Indians.

(p) **"Verified request"** means the process through which a consumer may submit a request to exercise a right or rights set forth in this Act, and by which a controller can reasonably authenticate the request and the consumer making the request using reasonable means.

SMTC 42.5 Responsibility According to Role

42.5.1 This Act shall establish the following responsibilities:

(a) Controllers are responsible for meeting the obligations established under this Act;

(b) Processors are responsible under this Act for adhering to the instructions of the controller and assisting the controller to meet its obligations under this Act; and

(c) Processing by a processor is governed by Tribal law or policy, and/or a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

SMTC 42.6 Consumer Rights

42.6.1 Verified Requests to Controllers. Controllers shall facilitate verified requests to exercise the consumer rights set forth in this section.

42.6.2 Right to Know. Upon a verified request from a consumer, a controller must confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold and where personal data concerning the consumer is being processed by the controller. If also requested by the consumer, the controller must also provide the categories of third parties with whom a controller shares personal data or to whom a controller sells personal data.

42.6.3 Right to Portability. Upon a verified request from a consumer, a controller must, in a commonly usable form, provide to the consumer, if technically feasible and reasonable, a copy of the personal data that the controller maintains about that consumer.

42.6.4 Right to Deletion. Upon a verified request from a consumer, a controller must delete the consumer's personal data that the controller maintains in identifiable form if one of the following grounds applies:

(a) The personal data is no longer necessary for a business purpose, including the provision of a product or service to the consumer;

(b) The consumer objects to the processing of his or her personal data and there are no business purposes related to (i) processing the personal data for the controller, (ii) the consumer whose personal data is being processed, or (iii) the public, for which the processing is necessary;

(c) The personal data has been unlawfully processed; or

(d) The personal data must be deleted to comply with a legal obligation under federal, state, local, or Tribal law to which the controller is subject.

This section does not apply to the extent processing is necessary:

1. For exercising the right of free speech;

2. For complying with a legal obligation;

3. To identify and repair errors that impair existing intended functionality;

4. For public interest, scientific or historical research purposes, or statistical purposes, where the deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing;

5. For the establishment, exercise, or defense of legal claims;

6. To detect or respond to security incidents; enable disaster recovery; protect against malicious, deceptive, fraudulent, or illegal activity; or identify, investigate, or prosecute those responsible for that activity;

7. For purposes of fulfilling or performing a contract or agreement with a consumer;

8. For internal or anticipated uses that are compatible and within the context for which the personal data is provided; or

9. For targeted advertising, so long as the controller provides the ability to opt-out of targeted advertising using either the opt-out provided by the Digital Advertising Alliance or the Network Advertising Initiative.

42.6.5 Right to Opt-Out of the Sale of Information. Using a "Do Not Sell My Personal Information" or "Do Not Sell My Personal Data" link, a button or e-mail request form or a physical form to be filled out in person, a consumer may direct a controller, at any time, not to sell the consumer's personal data to a third party. This may be referred to as the "right to opt-out." Notwithstanding the foregoing or any other provision of this Act, a controller shall not sell the personal data of a child under the age of 16, unless the child's parent or guardian has consented to the sale of the child's personal data. This may be referred to as the "right to opt-in."

42 6.6 Communication to Processors and Third Parties. A controller must communicate any correction, deletion, or restriction of processing carried out in accordance with sections 42.6.3, 42.6.4, or 42.6.5 of this section to each processor and third party recipient to whom the controller knows the personal data has been disclosed, unless this proves functionally impractical, technically infeasible, or involves disproportionate effort, or the controller knows or is informed by the third party that the third party is not continuing to use the personal data.

42.6.7 Action on Verified Request. A controller must provide information on action taken on a verified request under sections 42.6.2 through 42.6.6 of this section within sixty (60) days of receipt of the request. That period may be extended by sixty (60) additional days where reasonably necessary, taking into account the complexity and number of the requests. The controller must inform the consumer of any such extension within thirty (30) days of the request.

(a) If a controller does not take action on the request of a consumer, the controller must inform the consumer without undue delay and at the latest within forty-five days of receipt

of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) Information provided under this section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request.

(c) Upon any alleged violation of the provisions in this section, a consumer shall submit an administrative complaint to the Tribe, in a format to be provided by the Tribe, for determination of the appropriate remedy. If not satisfied with such determination, within thirty (30) days of receipt of such determination, the consumer may appeal the determination to the San Manuel Tribal Court, which shall have exclusive jurisdiction to review such determination. If issued a prevailing judgment by the San Manuel Tribal Court, a consumer shall only be entitled to injunctive relief specific to the processing of his or her personal data and nothing shall entitle the consumer to attorneys' or other fees, costs, money damages, punitive damages, or any other relief of any kind or for any purpose. Nothing in this Act shall be deemed to waive the sovereign immunity or permit claims or actions of any type against the Tribe or its affiliates or any of the elected officials, officers, directors, members, individual members of the General Council, managers, employees, representatives, contractors, or agents of the foregoing, except for the purposes and to the extent necessary before the Tribal Court to carry out this subsection (c). The foregoing limited waiver shall not be deemed to waive the Tribe's or any of its affiliates' sovereign immunity with respect to any assets of the Tribe or of its affiliates.

SMTC 42.7 Transparency

42.7.1 Controllers must be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that includes:

(a) The categories of personal data collected by the controller;

(b) The purposes for which the categories of personal data are used and disclosed to third parties, if any;

(c) The rights that consumers may exercise pursuant to section SMTC 42.6 of this Act, if any;

(d) The categories of personal data that the controller shares with third parties, if any; and

(e) The categories of third parties, if any, with whom the controller shares personal data.

42.7.2 If a controller sells personal data or processes personal data for targeted advertising, it must disclose such processing, as well as the manner in which a consumer may exercise the right to opt-out of such processing, in a clear and conspicuous manner.

SMTC 42.8 Exemptions

42.8.1 The obligations imposed on controllers or processors do not apply in those instances where compliance with this Act would restrict the Tribe's ability to:

(a) Comply with Tribal, federal, state, or local laws, rules, or regulations;

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by Tribal, federal, state, local, or other governmental authorities;

(c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate Tribal, federal, state, or local law;

(d) Investigate, exercise, or defend legal claims;

(e) Prevent or detect identify theft, fraud, or other criminal activity or verify identities;

(f) Perform a contract to which the consumer is a party or in order to take steps at the request of the consumer prior to entering into a contract;

(g) Protect the vital interests of the consumer or of another natural person;

(h) Perform a task carried out in the public interest;

(i) Process personal data of a consumer for one or more specific purposes where the consumer has given their consent to the processing; or

(j) Prevent, detect, or respond to security incidents, identify theft, fraud, harassment, malicious or deceptive activities, or any Illegal activity; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for any such action.

42.8.2 The obligations imposed on controllers or processors under this Act do not apply where compliance by the controller or processor with this Act would violate an evidentiary privilege under applicable law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under applicable law.

42.8.3 This Act does not require a controller or processor to do the following:

(a) Reidentify deidentified data;

(b) Retain, link, or combine personal data concerning a consumer that it would not otherwise retain, link, or combine in the ordinary course of business; or

(c) Comply with a request to exercise any of the rights under section SMTC 42.6 of this Act if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

42.8.4 This Act does not apply to:

(a) Personal data protected by the Gramm Leach Bliley Act or the Health Insurance Portability and Accountability Act of 1996;

(b) Personal data collected or maintained for purposes of the "Know Your Customer" and anti-money laundering laws of the United States; or

(c) Personal data collected or maintained under the Telephone Consumer Protection Act of 1991 (TCPA).

SMTC 42.9 Severability

42.9.1 In the event any provision of this Act is found to be invalid or unenforceable for any reason, such determination shall not affect the remaining terms.

SMTC 42.10 Effective Date

42.10.1 This Act, upon enactment by the General Council, shall be effective on January 1, 2020. The provisions of this Act shall apply to any dispute arising from or related to the subject matter hereof on or after the effective date of the Act.