CHAPTER 42. SAN MANUEL COMMERCIAL PRIVACY ACT[1]

YSMNC 42.1 Short Title

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

YSMNC 42.2 Findings

42.2.1 The Yuhaaviatam of San Manuel Nation (the "Nation") is a sovereign, federally recognized Indian tribe with inherent jurisdiction over the lands of the San Manuel Reservation and other lands, title to which is held by the United States of America in trust for the benefit of the Yuhaaviatam of San Manuel Nation, however previously referenced or denominated (collectively, "Tribal Trust Lands").

42.2.2 The Nation makes the following findings with respect to individual privacy and the Processing of Personal Data collected for Business Purposes from persons located on Tribal Trust Lands:

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

(b) The Nation and its Affiliates routinely collect Personal Data for governmental and Business Purposes.

(c) The Nation desires to provide individuals with a process to understand what type of Personal Data has been collected on Tribal Trust Lands for Business Purposes 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 Nation 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 for Business Purposes.

YSMNC 42.3 Purposes

42.3.1 This Act is adopted by the Nation, acting through the Tribal Authorities in the exercise of its inherent sovereign power to enact Tribal laws and otherwise safeguard and provide for the health and welfare of the Nation, its Tribal 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 Nation and its

[1] Adopted by the General Council on November 12, 2019. Amended by the Tribal Authorities on October 8, 2024.

Affiliates as Controllers and Processors of Data Subject Personal Data collected on Tribal Trust Lands for Business Purposes and the rights of Data Subjects with respect to such collected Personal Data.

42.3.3 This Act applies to the Processing of Personal Data wholly or partly by automated means and to the Processing other than by automated means of Personal Data which form part of a data repository or document management system or other database.

42.3.4 This Act does not apply to the Processing of Personal Data

(a) In the course of any activity which falls outside the scope of Tribal law;

(b) By a natural person in the course of a purely personal, family or household activity;

(c) By the Nation in the course of providing services to Tribal Citizens or members of the tribal community;

(d) By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety; or

(e) Undertaken for the purpose of meeting legal and regulatory requirements.

YSMNC 42.4 Definitions

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

(a) **"Act"** means this San Manuel Commercial Privacy Act, as may be amended.

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

(c) **"Biometric Data"** means an individual's physiological, biological, or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity. Biometric Data includes, but is not limited to, photographs, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(d) **"Business Purposes"** 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 Data Subject counting advertisement impressions, verifying positioning and quality of advertisement impressions, and auditing compliance with this specification and other standards;

(ii) Helping to ensure, investigate and/or restore security and integrity to the extent the use of the Data Subject's Personal Data is reasonably necessary and proportionate for these purposes;

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

(iv) Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a Data Subject's current interaction with the Controller, provided that the Data Subject's Personal Data is not disclosed to another Third Party and is not used to build a profile about a Data Subject or otherwise alter an individual Data Subject's experience outside the current interaction with the Controller;

(v) Performing services on behalf of the Controller, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing financing;

(vi) Providing advertising and marketing services, except for Targeted Advertising, to the Data Subject provided that, for the purpose of advertising and marketing, a Processor shall not combine the Personal Data of opted-out Data Subjects that the Processor receives from, or on behalf of, the Controller with Personal Data that the Processor receives from, or on behalf of, another person or persons or collects from its own interaction with Data Subjects;

(vii) Administering a club program with related rewards and premium features;

(viii) Entering into and/or administering an employment or independent contractual relationship with the Controller;

(ix) Undertaking internal research for technological development;

(x) Authenticating a Data Subject's identity;

(xi) Protecting the health and welfare of the Nation, its Affiliates, and individuals on Tribal Trust Lands; or

(xii) Ensuring regulatory obligations are satisfied.

(e) **"Consent"** means a clear affirmative act signifying a specific, informed, and unambiguous indication of a Data Subject's agreement to the Processing of Personal Data relating to the Data Subject, such as by a written statement or other clear affirmative action, provided that hovering over, muting, pausing or closing a given piece of content shall not constitute Consent, nor shall agreement obtained through use of Dark Patterns constitute Consent.

(f) **"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 Nation or its Affiliate(s) may be deemed a "Controller" or "Processor" (as defined below) as applicable.

(g) **"Dark Pattern"** means a user interface designed or manipulated with the

substantial effect of subverting or impairing user autonomy, decision-making, or choice.

(h) **"Data Subject"** means a natural person to whom Personal Data relates, who is a resident of the State of California or Tribal Trust Lands and whose Personal Data is collected by the Nation or by its Affiliates who are controlled by Tribal law, and includes Personal Data collected from a natural person acting in a commercial or employment context.

(i) **"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.

(j) **"Exempt Data"** means:

(i) Deidentified Data;

(ii) Publicly Available Information;

(iii) Lawfully obtained, truthful information that is a matter of public concern;

(iv) Any type of Personal Data listed in YSMNC 42.8.4.

(k) **"Identified or Identifiable Individual"** means a natural person who can be readily identified.

(l) **"Infer"** means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(m) **"Opt-Out Preference Signal"** means:

(i) The Global Privacy Control signal as described at https://globalprivacycontrol.org/; or

(ii) Any other widely known and recognized signals that are sent by a platform, technology, or mechanism, which communicates a Data Subject's choice to opt-out of the sale and sharing of Personal Data in a format commonly used and recognized by businesses, such as an HTTP header field or JavaScript object.

(n) **"Personal Data"** means any information that is linked or reasonably linkable to an Identified or Identifiable Individual. Personal Data does not include Exempt Data.

(o) **"Precise Geolocation"** means information derived from technology, including but not limited to global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of a natural person with precision and

accuracy within a radius of 1,850 feet. "Precise Geolocation" does not include the content of communications, or any data generated by or connected to the Nation's advanced utility metering infrastructure systems or equipment for use by a Tribal utility.

(p) **"Process"** or **"Processing"** means any collection, use, storage, disclosure, analysis, deletion, or modification of Personal Data, but excluding any activities constituting Targeted Advertising.

(q) **"Processor"** means a natural or legal person that Processes Personal Data on behalf of the Controller pursuant to a written contract that permits the Controller to audit the Processor's compliance with the contract through measures, including, but not limited to, regular assessments, and prohibits the person from:

(i) Selling or Sharing the Personal Data;

(ii) Retaining, using, or disclosing the Personal Data for any purpose other than to provide the services described in the contract with the Controller;

(iii) Retaining, using, or disclosing the Personal Data outside of the direct business relationship between the Processor and the Controller;

(iv) Combining the Personal Data received from, or on behalf of, the Controller with Personal Data that it receives from, or on behalf of, another natural or legal person or persons, or collects from its own interaction with the Data Subject except to the extent combining such Personal Data relates to providing the services to the Controller.

(r) **"Publicly Available Information"** means information that is lawfully made available from federal, state, Tribal, or local government records; information that the Processor or Controller has a reasonable basis to believe is lawfully made available to the general public by the Data Subject or from widely distributed media; or information made available by a person to whom the Data Subject has disclosed the information if the Data Subject has not restricted the information to a specific audience.

(s) **"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.

(t) **"Sale"** does not include the following:

(i) The disclosure of Personal Data to a Processor who Processes the Personal Data solely on behalf of the Controller;

(ii) The disclosure of Personal Data to a Third Party with whom the Data Subject 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.

(u) **"Sensitive Data"** means the following types of Personal Data:

(i) A Data Subject's social security, driver's license, state identification card, Tribal identification card, passport, or other government identification number;

(ii) A Data Subject's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;

(iii) A Data Subject's Precise Geolocation;

(iv) A Data Subject's racial or ethnic origin, religious or philosophical beliefs, or union membership;

(v) The contents of a Data Subject's mail, email, and text messages unless the Controller is the intended recipient of the communication;

(vi) A Data Subject's genetic data;

(vii) A Data Subject's Biometric Data processed for the purpose of unique identification;

(viii) Personal Data concerning a Data Subject's health; or

(ix) Personal Data concerning a Data Subject's sex life or sexual orientation.

(v) **"Share," "Shared,"** or **"Sharing"** means sharing, renting, releasing, disclosing, disseminating, making available, or otherwise communicating orally, in writing, or by electronic or other means, a Data Subject's Personal Data for Targeted Advertising. "Share," "Shared," or "Sharing," whether or not for monetary or other valuable consideration, does not include the following:

(i) A Data Subject's use or direction of the Controller to intentionally disclose Personal Data or intentionally interact with one or more Third Parties;

(ii) The Controller's use or sharing of an identifier for a Data Subject to alert the recipient that the Data Subject has exercised their right to opt-out of sharing or to limit the use of their Sensitive Data; or

(iii) 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.

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

(x) **"Third Party"** means a natural or legal person other than the Data Subject, Controller, Processor, or an Affiliate or Processor of the Processor or of the Controller.

(y) **"Tribal"** when capitalized, means of or relating to the Yuhaaviatam of San Manuel Nation.

(z) **"Tribal Authorities"** means the Governing Council collectively with a General Assembly, pursuant to the Yuhaaviatam of San Manuel Nation Constitution.

(aa) **"Tribal Citizen"** means a duly enrolled citizen of the Yuhaaviatam of San Manuel Nation.

(bb) **"Tribal Court"** means the San Manuel Tribal Court, established by the Yuhaaviatam of San Manuel Nation Constitution. The Tribal Court shall consist of a Supreme Court, the Appellate Court, the Trial Court, and such other inferior courts and dispute resolution forums as may be established by the Governing Council in the San Manuel Judicial Code, as amended.

(cc) **"Tribal Trust Lands"** means all land held in trust by the United States of America for the benefit of Yuhaaviatam of San Manuel Nation, however previously referenced or denominated.

(dd) **"Verified Request"** means the process through which a Data Subject 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 Data Subject making the request using reasonable means.

YSMNC 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 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.

YSMNC 42.6 Data Subject Rights

42.6.1 Verified Requests to Controllers. Controllers shall facilitate Verified Requests to exercise the Data Subject rights set forth in this section. Controllers shall ensure individuals responsible for handling Data Subject inquiries about the Controller's privacy practices or the Controller's compliance with this Act are informed of all requirements in this section, YSMNC 42.6, and how to direct Data Subjects to exercise their rights described in this section.

42.6.2 Right to Know. Upon a Verified Request from a Data Subject, a Controller must confirm whether or not Personal Data concerning the Data Subject is being Processed by the Controller, including whether such Personal Data is Sold and where Personal Data concerning the Data Subject is being Processed by the Controller. If also requested by the Data Subject, the Controller must also provide the categories of Third Parties with whom a Controller discloses Personal Data or to whom a Controller Sells or Shares Personal Data.

42.6.3 Right to Portability. Upon a Verified Request from a Data Subject, a Controller must, in a commonly usable form, provide to the Data Subject, if technically feasible and reasonable, a copy of the Personal Data that the Controller maintains about that Data Subject.

42.6.4 Right to Correct. Upon a Verified Request from a Data Subject that has provided evidence that any of Data Subject's Personal Data retained by the Controller is inaccurate, a Controller must use reasonable efforts to correct the inaccurate Personal Data as directed by the Data Subject.

42.6.5 Right to Deletion.

(a) Upon a Verified Request from a Data Subject, a Controller must delete the Data Subject's Personal Data that the Data Subject provided to Controller and the Controller maintains in identifiable form if one of the following grounds applies:

(i) The Personal Data is no longer necessary for a Business Purpose, including the provision of a product or service to the Data Subject;

(ii) The Data Subject 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 Data Subject whose Personal Data is being Processed, or (iii) the public, for which the Processing is necessary;

(iii) The Personal Data has been unlawfully Processed; or

(iv) 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.

(b) This section does not apply to the extent Processing is necessary:

(i) For exercising the right of free speech;

(ii) For complying with a legal obligation;

(iii) To identify and repair errors that impair existing intended functionality;

(iv) 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;

(v) For the establishment, exercise, or defense of legal claims;

(vi) 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 such activity;

(vii) For purposes of fulfilling or performing a contract or agreement with a Data Subject;

(viii) For internal or anticipated uses that are compatible and within the context for which the Personal Data is provided; or

(ix) For regulatory purposes.

42.6.6 Right to Limit the Use of Sensitive Data. If the Controller Processes Sensitive Data to Infer characteristics about the Data Subject, the Data Subject has a right to limit the use of their Sensitive Data by submitting a request via a "Limit the Use of My Sensitive Data" link, an email, or a physical form. A Controller that receives such a request must stop processing Sensitive Data to Infer characteristics, but the Controller may continue to Process Sensitive Data for other purposes, including to provide a product or service requested by the Data Subject. This may be referred to as the "Right to Limit." Sensitive Data that is collected or processed without the purpose of Inferring characteristics about a Data Subject is not subject to this section.

42.6.7 Right to Opt-Out of the Sale or Sharing of Personal Data. Using a "Do Not Sell or Share My Personal Data" link, an Opt-Out Preference Signal, a button or email request form, or a physical form to be filled out in person, a Data Subject may direct a Controller, at any time, not to Sell or Share the Data Subject'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 or Share 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.

42.6.8 Right to No Retaliation for Exercise of Rights. A Controller shall not discriminate or retaliate against a Data Subject because the Data Subject exercised any of the Data Subject's rights under this Act.

42.6.9 Communication to Processors and Third Parties. A Controller must communicate any request carried out in accordance with sections 42.6.3, 42.6.4, 42.6.5, or 42.6.6 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.

42.6.10 Action on Verified Request. A Controller must confirm receipt of a Verified Request within ten (10) days of receipt. A Controller must provide information on action taken on a Verified Request under sections 42.6.2 through 42.6.7 of this section within forty-five (45) days of receipt of the Verified Request. That period may be extended by forty-five (45) additional days where reasonably necessary, taking into account the complexity and number of the requests. The Controller must inform the Data Subject of any such extension within forty-five (45) days of the receipt of the Verified Request.

(a) If a Controller does not take action on the request of a Data Subject, the Controller must inform the Data Subject without undue delay 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 Data Subject. Where requests from a Data Subject 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 or section 42.10 herein, a Data Subject shall submit an administrative complaint to the Nation, in a format to be provided by the Nation, for determination of the appropriate remedy by the commission or agency designated by the Nation to render such administrative decisions. If not satisfied with such determination, within thirty (30) days of receipt of such determination, the Data Subject may appeal the determination to the San Manuel Tribal Court, which shall have exclusive jurisdiction to review such determination and shall adjudicate the appeal as an administrative review case limited in scope to the administrative record prepared by the designated commission or agency. If issued a prevailing judgment by the San Manuel Tribal Court, a Data Subject shall only be entitled to injunctive relief specific to the Processing of his or her Personal Data. Nothing shall entitle the Data Subject to attorneys' fees 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 of, or permit claims or actions of any type against, the Nation or its Affiliates or any of the elected officials, officers, directors, Tribal Citizens, managers, employees, representatives, contractors, or agents of the foregoing, except for the purposes and to the extent necessary before the San Manuel Tribal Court to carry out this subsection (c). The foregoing shall not be deemed to waive the Nation's or any of its Affiliates' sovereign immunity with respect to any assets of the Nation or of its Affiliates.

YMSNC 42.7 Transparency and Notice

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 Data Subjects a clear, meaningful privacy policy that includes:

(a) The categories of Personal Data collected by the Controller;

(b) The categories of sources from which the Data Subjects' Personal Data is collected;

(c) The purposes for which the categories of Personal Data are collected, used, disclosed, Shared or Sold to Third Parties, if any;

(d) The rights that Data Subjects may exercise pursuant to section YSMNC 42.6 of this Act, if any;

(e) The categories of Personal Data that the Controller discloses to Third Parties, if any; and

(f) The categories of Third Parties, if any, to whom the Controller discloses Personal

Data.

42.7.2 If a Controller Sells Personal Data or Shares Personal Data for Targeted Advertising, it must disclose such Processing, as well as the manner in which a Data Subject may exercise the right to opt-out of such Processing, in a clear and conspicuous manner. If a Controller obtains a Data Subject's Consent to Share or Sell Personal Data, it must not use any Dark Patterns to obtain such Consent.

42.7.3 If a Controller Processes Sensitive Data to Infer characteristics about the Data Subject, it must disclose such Processing, as well as the manner in which a Data Subject may exercise the right to limit such Processing, in a clear and conspicuous manner.

YSMNC 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 Nation's ability to:

(a) Comply with Tribal, federal, state, or local laws, rules, or regulations as may be applicable;

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

(c) Cooperate with law enforcement agencies concerning conduct or activity that the Controller or Processor reasonably and in good faith believes may violate applicable 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 Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

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

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

(i) Process Personal Data of a Data Subject for one or more specific purposes where the Data Subject 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 Data Subject to a natural or legal 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 Data Subject 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 YSMNC 42.6 of this Act if the Controller is unable to verify, using commercially reasonable efforts, the identity of the Data Subject 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;

(c) Data Subject Personal Data collected or maintained for purposes of the Fair Credit Reporting Act (FCRA); or

(d) Personal Data collected or maintained under the Driver's Privacy Protection Act (DPPA).

YSMNC 42.9 Privacy Impact Assessment

42.9.1 Where the Processing of Personal Data is likely to result in a high risk to the Data Subject's rights and freedoms, the Controller must undertake and document a privacy impact assessment to evaluate the origin, nature, particularity and severity of that risk. Where a privacy impact assessment indicates the Processing operations involve a high risk which the Controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, the Processing operations should cease or not be undertaken.

YSMNC 42.10 Security

42.10.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing Data Subjects' Personal Information as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Controller and the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk to the Personal Information, including inter alia, as appropriate:

(a) The de-identification and encryption of Personal Data, including the use of multi-factor authentication and similar tools for access to Personal Data;

(b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(c) The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;

(d) A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

42.10.2 Upon any alleged violation of this Section 42.10, and only for purposes of this Section, the remedies set forth at Section 42.6.10.(c) shall apply to Personal Information, with "Personal Information" defined as either of the following:

(i) An individual's first name or first initial and the individual's last time in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

1. Social security number.

2. Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.

3. Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

4. Medical information. "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

5. Health insurance information. "Health insurance information" means an individual's insurance policy number or subscriber information number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeal records.

6. Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.

7. Genetic data. "Genetic data" means any data, regardless of its format, which results from the analysis of a biological sample of an individual, or

from another source enabling equivalent information to be obtained and concerns genetic material. Genetic material includes, but is not limited to, deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes, alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs), uninterpreted data that results from analysis of the biological sample or other source, and any information extrapolated, derived, or inferred therefrom.

(ii) A username or email address in combination with a password or security question and answer that would permit access to an online account.

(iii) "Personal Information" does not include Publicly Available Information that is lawfully made available to the general public from federal, state, or local government records.

YSMNC 42.11 Severability

42.11.1 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.

YSMNC 42.12 Tribal Sovereign Immunity

42.12.1 Subject to sections 42.6 and 42.10 herein, nothing contained within this Act shall be deemed to constitute a waiver or diminution of any type whatsoever of the Nation's sovereign immunity from unconsented suit, which sovereign immunity is hereby expressly reaffirmed. Nor may any provision of this Act be construed as consent to the assertion of power or authority by, or the application of any laws of, any other jurisdiction or entity.

YSMNC 42.13 Effective Date

42.13.1 This Act, upon enactment by the Tribal Authorities, shall be immediately effective as amended.