



## TUCKER & COMPANY

|                                                                           |                                                                                                                                                     |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy Title:</b>                                                      | <b>Privacy and Data Protection Policy</b>                                                                                                           |
| <b>Issuing Date:</b>                                                      | January 1, 2020                                                                                                                                     |
| <b>Effective Date:</b>                                                    | January 1, 2020                                                                                                                                     |
| <b>Review Frequency:</b>                                                  | Annual                                                                                                                                              |
| <b>Last Review Date:</b>                                                  | January 10, 2025                                                                                                                                    |
| <b>Revision Number:</b>                                                   | 1.1                                                                                                                                                 |
| <b>Subject Matter Experts:</b>                                            | Data Protection Officer<br>General Counsel<br>Senior Manager,<br>General Counsel<br>Data Protection Officer (DPO)<br>Chief Technology Officer (CTO) |
| <b>Policy Owner/Executive Approver:</b>                                   |                                                                                                                                                     |
| <b>Information Security Team/IEC 27001:<br/>2013 standards addressed:</b> | A.5 Security Policies<br>A.8.2.1 Classification of Information,<br>A.8.2.3 Handling of Assets                                                       |

### 1. Purpose

This policy sets forth the general principles to be applied by Tucker & Company (“Company”) to the collection, use, retention and/or disclosure of Personal Information (as defined below) relating to employees of the Company (“Employees”), temporary employees, contractors and consultants (collectively “Contractors”) and Company survey respondents (collectively “Respondents”). Please note that in certain jurisdictions, Personal Information may also include IP address. In addition to the requirements set forth in this Policy, use and/or disclosure of Personal Information may be governed by a confidentiality agreement with a third party so please consult with the Legal Department if you have any questions whether a certain use or disclosure of information is permitted.

### 2. Scope

The intent of this policy is to establish a common foundation for the processing and protection of Personal Information by the Company worldwide. For purposes of this policy, “processing” means any operation performed upon Personal Information, including, but not limited to, collecting, recording, storing, updating, modifying, retrieving, using, disclosing, transmitting, disseminating, combining, analyzing, erasing and/or destroying. This policy applies to all Personal Information contained in paper files and/or electronic format (including electronic mail and saved word document files). From time to time, certain countries, lines of business and/or subsidiaries may require additional policies and/or procedures to address legal requirements or business need.

### 3. Policy

#### 3.1. Collection and Processing

The Company will collect Personal Information only as permitted by law. Personal Information will be processed in accordance with applicable law, including CCPA regulations noted in Appendix A, and any applicable contractual obligations.



## TUCKER & COMPANY

### **3.2. Notice**

If required by law or contract, the Company will provide individuals with information regarding the processing of their Personal Information, the categories of information it stores, the recipients of such Personal Information and/or any other information necessary to process Personal Information in accordance with applicable law.

### **3.3. Consent**

If required by law or contract, the Company will seek consent of an individual prior to collecting, using or disclosing Personal Information.

### **3.4. Use and Retention**

The Company will process, store and disclose Personal Information only for business purposes and as permitted by law. Personal Information will be retained only for so long as permitted by law.

### **3.5. Safeguarding Personal Information**

The Company will establish safeguards to reasonably and appropriately protect Personal Information from unauthorized use, disclosure, destruction and/or alteration. In addition, the Company shall adopt a “clean desk” approach to treatment of Sensitive Personal Information. Employees and Contractors shall not write down Sensitive Personal Information, including but not limited to credit/debit account numbers, social security numbers and/or health information. If an Employee uses or has access to printed documents which include Sensitive Personal Information as part of his or her job responsibilities, such documents should be secured when not in use in a locked file cabinet, locked desk drawer or locked office and should be discarded in the confidential disposal boxes for shredding when no longer needed. Employees and Contractors shall not use Sensitive Personal Information for any reason other than to support his or her job responsibilities.

### **3.6. Processing Sensitive Information**

The Company will adopt additional measures relating to the processing of Sensitive Information. For purposes of this Policy, Sensitive Information shall include financial account information, social security or national identifier numbers, data relating to racial or ethnic origin, political views, religious or philosophical beliefs, trade union membership, data concerning health or sexual orientation and/or data relating to criminal convictions or similar offenses.

### **3.7. Quality**

The Company will undertake reasonable efforts to ensure that the Personal Information it holds is accurate, complete and otherwise reliable to the best of its knowledge.

### **3.8. Access**

If an individual requests access to Personal Information relating to him or her, requests that errors in his or her Personal Information be corrected and/or requests that information no longer needed for a legitimate business purpose be deleted, The Company will consider such requests and will comply where it is required by law to do so. Please direct all such requests to the Legal Department.



## TUCKER & COMPANY

### **3.9. Disclosures to Third Parties**

The Company will disclose Personal Information to third parties for business purposes only as permitted by law and, if the Personal Information relates to Respondents, in accordance with the terms of the privacy policy or relates disclosures provided to them at the time of data collection. Disclosure may require that the Company enter into an agreement with the recipient to require the recipient to undertake certain reasonable and adequate safeguards with respect to the Personal Information. Please consult the Legal Department to determine if an agreement is necessary prior to disclosing Personal Information outside of the Company.

### **3.10. International Transfers of Personal Information**

The Company may transfer Personal Information outside the country in which it is collected only for legitimate business purposes and only as permitted by law. Such transfer may require an agreement with the recipient, even if the recipient is another Company and/or another Company line of business. Please consult the Legal Department to determine if an agreement is necessary prior to transferring Personal Information outside of the country in which such Personal Information was collected.

### **4. Exceptions**

Exceptions to compliance with any part of this policy may pose a risk to the confidentiality, integrity, and availability and privacy of Tucker & Company Information Systems and Data and may only be approved by the DPO and Legal department and suitably documented. Questions regarding this Policy should be directed to the Legal Department.

### **5. Awareness and Enforcement**

Tucker & Company will undertake reasonable efforts to help ensure that Workforce Members are aware of and comply with the terms of this Policy. Noncompliance with the Policy may result in disciplinary actions up to and including termination and/or may result in liability to Tucker & Company pursuant to applicable law or contract.

### **6. Definitions**

Please refer to the Information Security Glossary for general definitions.

Personal Information includes any information that relates to an identifiable natural person which includes, but is not limited to, name, mailing address, telephone number, electronic mail address, social security number, social insurance number or any other national identifier, financial information (including credit and/or debit account information), driver's license number, state identification card number, passport number, alien registration number, health insurance identification number, age, gender, marital status and/or personal or family income.

### **7. Change and Version Control Manifest**

All changes to this document require proper log documentation to ensure the quality of change and version control. To note revisions to this document, enter the information into the table below as outlined.

- V # (version #) -- the version number of the document to which revisions were applied.
- Rev Date (revision date) – the date of the revision request.
- Summary of Revisions – description of the revisions being made and sections affected.



TUCKER & COMPANY

- Rev By (revisions by) – the Technical Writer or assigned Workforce Member who is responsible for making revisions.
- App By (approved by) – the person(s) who must provide approval for the revision and re-issuance or re-publication of the procedure.
- App Date (date approved) – the date the person(s) approved the revision.



## TUCKER & COMPANY

### Appendix A – CCPA regulations

CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS Article 1. GENERAL PROVISIONS § 999.300. Title and Scope. (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have. (b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155 and 1798.185, Civil Code. § 999.301. Definitions. In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations: (a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer’s personal information in accordance with the methods set forth in section 999.330. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. (b) “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General. (c) “Authorized agent” means a natural person or a business entity registered with the Secretary of State to conduct business in California that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326. (d) “Categories of sources” means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers. (e) “Categories of third parties” means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers. (f) “CCPA” means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 et seq. (g) “COPPA” means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to 6508 and 16 Code of Federal Regulations part 312.5. (h) “Employment benefits” means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer’s employer. (i) “Employment-related information” means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision (h)(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a business purpose. (j) “Financial incentive” means a program, benefit, or other offering, including payments to consumers, related to the collection, deletion, or sale of personal information. (k) “Household” means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier. (l) “Notice at collection” means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these



## TUCKER & COMPANY

regulations. (m) “Notice of right to opt-out” means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations. (n) “Notice of financial incentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations. (o) “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, or sale of personal information, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, or sale of personal information, including the denial of goods or services to the consumer. (p) “Privacy policy,” as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business’s practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information, and of the rights of consumers regarding their own personal information. (q) “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105. (r) “Request to know” means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following: (1) Specific pieces of personal information that a business has collected about the consumer; (2) Categories of personal information it has collected about the consumer; (3) Categories of sources from which the personal information is collected; (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer; (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and (6) The business or commercial purpose for collecting or selling personal information. (s) “Request to opt-in” means the affirmative authorization that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age, by a consumer at least 13 and less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information. (t) “Request to opt-out” means a consumer request that a business not sell the consumer’s personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a). (u) “Signed” means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 et seq. (v) “Third-party identity verification service” means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete. (w) “Value of the consumer’s data” means the value provided to the business by the consumer’s data as calculated under section 999.337. (x) “Verify” means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer’s parent or legal guardian. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145 and 1798.185, Civil Code. Article 2. NOTICES TO CONSUMERS § 999.304. Overview of Required Notices. (a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 999.308. (b) A business that collects personal information from a consumer shall provide a notice at collection in accordance with the CCPA and section 999.305. (c) A business that sells personal information shall provide a notice of right to opt-out in accordance with the



## TUCKER & COMPANY

CCPA and section 999.306. (d) A business that offers a financial incentive or price or service difference shall provide a notice of financial incentive in accordance with the CCPA and section 999.307. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.115, 1798.120, 1798.125, 1798.130 and 1798.135, Civil Code. § 999.305. Notice at Collection of Personal Information. (a) Purpose and General Principles (1) The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used. (2) The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall: a. Use plain, straightforward language and avoid technical or legal jargon. b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable. c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California. d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format. (3) The notice at collection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow: a. When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected. b. When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu. c. When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online. d. When a business collects personal information over the telephone or in person, it may provide the notice orally. (4) When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection. (5) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection. (6) If a business does not give the notice at collection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer. (b) A business shall include the following in its notice at collection: (1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected. (2) The business or commercial purpose(s) for which the categories of personal information will be used. (3) If the business sells personal information, the link titled "Do Not Sell My Personal Information" required by section 999.315, subsection (a), or in the case of offline notices, where the webpage can be found online. (4) A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be



## TUCKER & COMPANY

found online. (c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business's privacy policy that contains the information required in subsection (b). (d) A business that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information. (e) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq. does not need to provide a notice at collection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out. (f) A business collecting employment-related information shall comply with the provisions of section 999.305 except with regard to the following: (1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information". (2) The notice at collection of employment-related information is not required to provide a link to the business's privacy policy. (g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise. Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115 and 1798.185, Civil Code. § 999.306. Notice of Right to Opt-Out of Sale of Personal Information. (a) Purpose and General Principles (1) The purpose of the notice of right to opt-out is to inform consumers of their right to direct a business that sells their personal information to stop selling their personal information. (2) The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall: a. Use plain, straightforward language and avoid technical or legal jargon. b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable. c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California. d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format. (b) A business that sells the personal information of consumers shall provide the notice of right to opt-out to consumers as follows: (1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" link on the website homepage or the download or landing page of a mobile application. In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu. The notice shall include the information specified in subsection (c) or link to the section of the business's privacy policy that contains the same information. (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out. That method shall comply with the requirements set forth in subsection (a)(2). (c) A business shall include the following in its notice of right to opt-out: (1) A description of the consumer's right to opt-out of the sale of their personal information by the business; (2) The interactive form by which the consumer can submit their request to opt-out online, as required by section 999.315, subsection (a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out; and (3) Instructions for any other method by which the consumer may submit their request to opt-out. (d) A business does not need to provide a notice of right to opt-out if: (1) It does not sell personal information; and (2) It states in its privacy policy that it does not sell personal information. (e) A business shall not sell the personal information it collected during the time the business did not have a notice of right to





## TUCKER & COMPANY

opt-out posted unless it obtains the affirmative authorization of the consumer. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code. § 999.307. Notice of Financial Incentive. (a) Purpose and General Principles (1) The purpose of the notice of financial incentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a notice of financial incentive. (2) The notice of financial incentive shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall: a. Use plain, straightforward language and avoid technical or legal jargon. b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable. c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California. d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format. e. Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. (3) If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b). (b) A business shall include the following in its notice of financial incentive: (1) A succinct summary of the financial incentive or price or service difference offered; (2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data; (3) How the consumer can opt-in to the financial incentive or price or service difference; (4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and (5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including: a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and b. A description of the method the business used to calculate the value of the consumer's data.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code. § 999.308. Privacy Policy. (a) Purpose and General Principles (1) The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. (2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers. The policy shall: a. Use plain, straightforward language and avoid technical or legal jargon. b. Use a format that makes the policy readable, including on smaller screens, if applicable. c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California. d. Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format. e. Be available in a format that allows a consumer to print it out as a document. (b) The privacy policy shall be posted online through a conspicuous link using the word



## TUCKER & COMPANY

“privacy” on the business’s website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers’ privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application’s settings menu. (c) The privacy policy shall include the following information: (1) Right to Know About Personal Information Collected, Disclosed, or Sold. a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells. b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business. c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide. d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected. e. Identification of the categories of sources from which the personal information is collected. f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold. g. Disclosure or Sale of Personal Information. 1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months. 2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold. 3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age. (2) Right to Request Deletion of Personal Information. a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business. b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business. c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide. (3) Right to Opt-Out of the Sale of Personal Information. a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business. b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 999.306. (4) Right to Non-Discrimination for the Exercise of a Consumer’s Privacy Rights. a. Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA. (5) Authorized Agent. a. Instructions on how an authorized agent can make a request under the CCPA on the consumer’s behalf. (6) Contact for More Information. a. A contact for questions or concerns about the business’s privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer. (7) Date the privacy policy was last updated. (8) If subject to the requirements set forth in section 999.317, subsection (g), the information compiled in section 999.317, subsection (g)(1), or a link to it. (9) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 999.330 and 999.331. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code. Article 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS § 999.312. Methods for Submitting Requests to Know and Requests to Delete. (a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to know. All other businesses shall provide two or



## TUCKER & COMPANY

more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail. (b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail. (c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number. (d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted. (e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either: (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code. § 999.313. Responding to Requests to Know and Requests to Delete. (a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 business days and provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call. (b) Businesses shall respond to requests to know and requests to delete within 45 calendar days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request. (c) Responding to Requests to Know. (1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2). (2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of



## TUCKER & COMPANY

personal information set forth in its privacy policy. (3) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met: a. The business does not maintain the personal information in a searchable or reasonably accessible format; b. The business maintains the personal information solely for legal or compliance purposes; c. The business does not sell the personal information and does not use it for any commercial purpose; and d. The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above. (4) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data. (5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer. (6) A business shall use reasonable security measures when transmitting personal information to the consumer. (7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4. (8) Unless otherwise specified by the business to cover a longer period of time, the 12month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request. (9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories. (10) In responding to a verified request to know categories of personal information, the business shall provide: a. The categories of personal information the business has collected about the consumer in the preceding 12 months; b. The categories of sources from which the personal information was collected; c. The business or commercial purpose for which it collected or sold the personal information; d. The categories of third parties with whom the business shares personal information; e. The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and f. The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information. (11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed. (d) Responding to Requests to Delete. (1) For



## TUCKER & COMPANY

requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified. (2) A business shall comply with a consumer's request to delete their personal information by: a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems; b. Deidentifying the personal information; or c. Aggregating the consumer information. (3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose. (4) In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. (5) If the business complies with the consumer's request, the business shall inform the consumer that it will maintain a record of the request as required by section 999.317, subsection (b). A business may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's records. (6) In cases where a business denies a consumer's request to delete, the business shall do all of the following: a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, unless prohibited from doing so by law; b. Delete the consumer's personal information that is not subject to the exception; and c. Not use the consumer's personal information retained for any other purpose than provided for by that exception. (7) If a business that denies a consumer's request to delete sells personal information and the consumer has not already made a request to opt-out, the business shall ask the consumer if they would like to opt-out of the sale of their personal information and shall include either the contents of, or a link to, the notice of right to opt-out in accordance with section 999.306. (8) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered and more prominently presented than the other choices. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code. § 999.314. Service Providers. (a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations. (b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations. (c) A service provider shall not retain, use, or disclose personal information obtained in the course of providing services except: (1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information, and in compliance with the written contract for services required by the CCPA; (2) To retain and employ another service provider as a subcontractor, where the subcontractor meets the requirements for a service provider under the CCPA and these regulations; (3) For internal use by the service provider to build or improve the quality of its services, provided that the use does not include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source; (4) To detect data security incidents or protect against fraudulent or illegal activity; or (5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(4). (d) A service



## TUCKER & COMPANY

provider shall not sell data on behalf of a business when a consumer has opted-out of the sale of their personal information with the business. (e) If a service provider receives a request to know or a request to delete from a consumer, the service provider shall either act on behalf of the business in responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider. (f) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code. § 999.315.

**Requests to Opt-Out.** (a) A business shall provide two or more designated methods for submitting requests to opt-out, including an interactive form accessible via a clear and conspicuous link titled “Do Not Sell My Personal Information,” on the business’s website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information. (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business sells personal information to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. (c) If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer. (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. (2) If a global privacy control conflicts with a consumer’s existing business-specific privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program. (d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sale for certain uses of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices. (e) A business shall comply with a request to opt-out as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. If a business sells a consumer’s personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer’s information. (f) A consumer may use an authorized agent to submit a request to opt-out on the consumer’s behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent cannot provide to the business the consumer’s signed permission demonstrating that they have been authorized by the consumer to act on the consumer’s behalf. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent. (g) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and



## TUCKER & COMPANY

documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code. § 999.316. Requests to Opt-In After Opting-Out of the Sale of Personal Information. (a) Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in. (b) If a consumer who has opted-out of the sale of their personal information initiates a transaction or attempts to use a product or service that requires the sale of their personal information, a business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can opt-in. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code. § 999.317. Training; Record-Keeping. (a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations. (b) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records. (c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part. (d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations. (e) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for recordkeeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation. (f) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA. (g) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall: (1) Compile the following metrics for the previous calendar year: a. The number of requests to know that the business received, complied with in whole or in part, and denied; b. The number of requests to delete that the business received, complied with in whole or in part, and denied; c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and d. The median or mean number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out. (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. a. In its disclosure pursuant to subsection (g)(2), a business may choose to disclose the number of requests that it denied in whole or in part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds. (3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA. (h) A business may choose to compile and disclose the information required by subsection (g)(1) for requests received from all



## TUCKER & COMPANY

individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (g)(1) for requests received from consumers. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135 and 1798.185, Civil Code. § 999.318. Requests to Know or Delete Household Information. (a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied: (1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information; (2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 999.325; and (3) The business verifies that each member making the request is currently a member of the household. (b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations. (c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 999.330. Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140 and 1798.185, Civil Code.

Article 4. VERIFICATION OF REQUESTS § 999.323. General Rules Regarding Verification. (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information. (b) In determining the method by which the business will verify the consumer's identity, the business shall: (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section. (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer. (3) Consider the following factors: a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive; b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process; c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be; d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated; e. The manner in which the business interacts with the consumer; and f. Available technology for verification. (c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required





## TUCKER & COMPANY

to comply with section 999.317. (d) A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to know or request to delete. For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization. (e) A business shall implement reasonable security measures to detect fraudulent identity verification activity and prevent the unauthorized access to or deletion of a consumer's personal information. (f) If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code. § 999.324. Verification for Password-Protected Accounts. (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data. (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code. § 999.325. Verification for Non-Account Holders. (a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 999.323. (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer. (c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations. (d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs may require a reasonably high degree of certainty, while the deletion of browsing history may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations. (e) Illustrative examples follow: (1) Example 1: If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they



## TUCKER & COMPANY

recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty. (2) Example 2: If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 999.323, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device. (f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations. (g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5). Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code. § 999.326. Authorized Agent. (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, a business may require that the consumer do the following: (1) Provide the authorized agent signed permission to do so. (2) Verify their own identity directly with the business. (3) Directly confirm with the business that they provided the authorized agent permission to submit the request. (b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4121 to 4130. (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information. (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code. Article 5. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE § 999.330. Consumers Under 13 Years of Age. (a) Process for Opting-In to Sale of Personal Information (1) A business that has actual knowledge that it sells the personal information of a consumer under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under COPPA. (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to: a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan; b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel; d. Having a parent or guardian connect to trained personnel via video-conference; e. Having a parent or guardian communicate in person with trained personnel; and f. Verifying a parent or guardian's identity by checking a form of government issued identification against databases of such information, as long as the



## TUCKER & COMPANY

parent or guardian's identification is deleted by the business from its records promptly after such verification is complete. (b) When a business receives an affirmative authorization pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out and of the process for doing so on behalf of their child pursuant to section 999.315, subsections (a)-(f). (c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to know or a request to delete the personal information of a child under the age of 13 is the parent or guardian of that child. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code. § 999.331. Consumers 13 to 15 Years of Age. (a) A business that has actual knowledge that it sells the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale of their personal information, pursuant to section 999.316. (b) When a business receives a request to opt-in to the sale of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code. § 999.332. Notices to Consumers Under 16 Years of Age. (a) A business subject to sections 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy. (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information without the affirmative authorization of consumers at least 13 years of age and less than 16 years of age, or the affirmative authorization of their parent or guardian for consumers under 13 years of age, is not required to provide the notice of right to opt-out. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code. Article 6. NON-DISCRIMINATION § 999.336. Discriminatory Practices. (a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations. (b) A business may offer a financial incentive or price or service difference if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive or price or service difference is reasonably related to the value of the consumer's data, that business shall not offer the financial incentive or price or service difference. (c) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory. (d) Illustrative examples follow: (1) Example 1: A music streaming business offers a free service as well as a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the \$5-per-month payment is reasonably related to the value of the consumer's data to the business. (2) Example 2: A clothing business offers a loyalty program whereby customers receive a \$5-off coupon by email after spending \$100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1). (3) Example 3: A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide



## TUCKER & COMPANY

their phone numbers. A consumer submits a request to opt-out of the sale of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business. (4) Example 4: An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business. (e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307. (f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (i)(3), shall not be considered a financial incentive subject to these regulations. (g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code. § 999.337. Calculating the Value of Consumer Data (a) A business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following: (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data. (2) The average value to the business of the sale, collection, or deletion of a consumer's data. (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers. (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information. (5) Expenses related to the sale, collection, or retention of consumers' personal information. (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference. (7) Profit generated by the business from sale, collection, or retention of consumers' personal information. (8) Any other practical and reasonably reliable method of calculation used in good faith. (b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers. Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.