TrustArc

CCPA Accountability HANDBOOK

A Comprehensive Compliance Guide for the California Consumer Privacy Act (CCPA)

Includes Full Text of the California Consumer Privacy Act of 2018

Introduction

On 1 January 2020, the California Consumer Privacy Act (CCPA) entered into application and broadly expands the rights of California consumers and requires companies within scope to be significantly more transparent about how they collect, use and disclose personal information. Enforcement of the law is slated to begin not later than 1 July 2020.

For companies doing business in California, this law is becoming a compelling event to invest heavily in privacy management throughout the organization. Given the new individual rights within the law (right to know; right to request deletion; and right to opt-out of sales of personal information), along with a private right of action where personal information is subject to an unauthorized access and exfiltration, theft or disclosure due to failure to implement and maintain reasonable security procedures and practices, the risk of non-compliance is significant.

For multi-jurisdictional companies, this represents one more law to comply with. Organizations that have been focusing on building an accountable privacy program or on comprehensive compliance initiatives for the European Union's General Data Protection Regulation (Regulation (EU) 2016/679, also known as the "GDPR") will be able to leverage that work for CCPA compliance initiatives.

This Handbook is designed to support the ability of the Privacy Office in operationalizing the privacy compliance obligations under the CCPA. It is also intended to help multi-jurisdictional organizations leverage their other privacy compliance initiatives, for example under the GDPR, to support CCPA compliance. It is organized in four parts:

- ***Part 1: California Consumer Privacy Act – Accountability Annotations and Operational Guide***
  In this section, TrustArc's Privacy Intelligence Team has analyzed the law and identified provisions that require the implementation of a policy, procedure, mechanism or other type of technical and organizational measure in order to demonstrate compliance or support compliance efforts.
- ***Part 2: An Accountability Approach to Demonstrating Compliance with the GDPR and CCPA***
  For organizations operating in multiple jurisdictions, this section identifies the specific Articles of the GDPR as well as the provisions of the CCPA where evidence of a privacy management activity (technical or organizational measure), mapped to the Framework, will achieve compliance. This will help organizations streamline and prioritize compliance
- initiatives within a privacy management program approach.

- ***Part 3: Complying with the California Consumer Privacy Act***
  This section will provide a more detailed background on what is required to comply with the CCPA and explains how TrustArc's software solutions can support your compliance efforts.
- ***Part 4: Full Text of the California Consumer Privacy Act of 2018***

PART 1

California Consumer Privacy Act –
Accountability Annotations and Operational Guide

Demonstrating Compliance with the CCPA

Demonstrating compliance with the CCPA means organizations will develop, implement and maintain appropriate policies, procedures and other measures that are necessary to be able to deal with the requirements of the law. On the following pages, you will find the overview of the provisions of the law, mapped to the privacy management activities from Nymity's Privacy Management Accountability Framework™ that have been identified as aiding in demonstrating legal compliance with the CCPA. In Part 2, you will see how Nymity's privacy management activities have been integrated into TrustArc's Privacy & Data Governance Framework to create a seamless experience for both Nymity and TrustArc customers.

The mapping of provisions of law to privacy management activities is structured as follows:

Accountability Annotation	Privacy Management Activities (Technical and Organizational Measures)	Example Accountability Mechanisms	Example Evidence
An annotation explaining the meaning and impact of the Section	A list of privacy management activities that once implemented may help: 1. Achieve ongoing compliance with the CCPA and, 2. Produce documentation that will help demonstrate compliance. In some cases, the measure may not be applicable to your organization.	A listing of possible policies, procedures, guidelines, checklists, training and awareness activities, transparency measures, technical safeguards and other mechanisms that may mitigate internal and external privacy risk. Accountability Mechanisms are produced when organizations put in place technical and organizational measures	A listing of sample evidence indicating that the accountability mechanisms have been implemented and used appropriately.

Accountability Annotation	Technical and Organizational Measures	Example Accountability Mechanisms	Example Evidence
1798.100 This section addresses consumers' right to request disclosure of categories and specific pieces of information businesses have collected about them. Businesses must inform consumers, before collection, of: ● categories of personal information to be collected; and ● purposes for which this personal information has been collected. Where personal information is requested, to the extent it is required to be disclosed, it should be in a portable format and, if technically feasible, capable of being transmitted to another entity by the individual.	**Maintain and implement procedures to provide for and respond to requests for access to personal data** This privacy management activity addresses the primary processes and procedures needed to ensure businesses can respond to access requests in a timely and appropriate manner. **Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for required information to be provided to consumers about collection and use of their personal information. **Maintain procedures to respond to requests for data portability** This privacy management activity ensures policies and procedures are in place to	Protocol or procedure for responding to access requests Access request form Template letters for responding to requests Access request log Procedures for responding to customer requests Customer service mailbox Policy or procedure for responding to requests for information Procedures for responding to customer requests and preferences Data privacy notice Policy or procedure for responding to requests for data portability	Documentation that workflows for request demonstrate that procedures are being followed Random audit of files that demonstrates that templates are used in communications with requestors Documentation that customer service mailbox is tested to verify it is monitored and responded to Log tracking requests validates that timelines for responses are met Audit results that protocols are being followed Copy of the information notice provided to consumers Documentation showing that privacy notice is aligned to legal requirements

The section also clarifies that personal information need not be retained if collected for single, one-time transactions if the information is not sold or otherwise retained by the business.	provide data subjects with their personal information in a portable, readily usable format for transmission to another entity. **Integrate data privacy into records retention practices** This privacy management activity helps the organization embed data privacy into the records retention schedule to ensure the proper storage of personal information. **Maintain policies/procedures for secondary uses of personal data** This privacy management activity addresses having policies and procedures that define how to handle situations when the organization wishes to use personal data beyond the primary purpose. **Additional privacy management activities that will help ensure policies and procedures are in place to respond to DSAR requests:**	Technical solution for processing data portability requests Records retention schedule Technical configurations that limit the storage of personal information Data privacy policy that prohibits the sale of personal information or secondary use of personal information in a manner not compatible with the purpose for which it was collected	Testing of technical solution validates that data is properly exported Audit results examining that the retention schedule was followed

	Maintain and implement procedures to provide for and respond to requests to opt-out of, restrict or object to processing Maintain and implement procedures to provide for and respond to requests and/or provide a mechanism for individuals to update or correct their personal data Maintain and implement procedures to provide for and respond to requests for information Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data		
1798.105 This section addresses consumers' right to request deletion of personal information. Exceptions include where personal information is maintained for:	**Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data** This privacy management activity addresses the primary processes and procedures needed to ensure personal information are deleted upon	Protocol or procedure for responding to deletion request Procedures for responding to customer requests Customer service mailbox Customer or user portal to update data	Audit results that the protocols are being followed Documentation that customer service mailbox is tested to verify it is monitored and responded to Test results for portal functionality

● transaction completion; ● detection of security incidents or protection against malicious, deceptive, fraudulent or illegal activity; ● debugging for identification and repair of functionality errors; ● exercise of free speech; ● compliance with the *California Electronic Communications Privacy Act*; ● engaging in scientific, historical or statistical research in the public interest; ● enabling solely internal uses reasonably aligned with consumer expectations; ● compliance with a legal obligation; or ● otherwise lawful use, compatible	request, where appropriate, in a timely and effective manner. **Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for required information to be provided to consumers about deletion of their personal information. **Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates)** This privacy management activity helps the organization determine what data protection requirements are needed for contracts with third-parties who receive the personal data from the organization. **Maintain procedures to execute contracts or agreements with all processors** This privacy management activity addresses steps taken	Data privacy notice Data privacy and security requirements for third parties Procurement policy Template contract language for privacy requirements Procedure/workflow for executing contracts	Copy of the information notice provided to consumers Documentation showing that privacy notice is aligned to legal requirements Contracts with third parties addressing requirements to delete personal information

with the context in which the consumer provided the information. The section also provides that businesses must direct service providers to also delete personal information from their records.	to ensure written or electronic contracts are in place with processors. **Additional privacy management activities that will help ensure policies and procedures are in place to respond to DSAR requests:** Maintain and implement procedures to provide for and respond to requests for access to personal data Maintain and implement procedures to provide for and respond to requests to opt-out of, restrict or object to processing Maintain and implement procedures to provide for and respond to requests and/or provide a mechanism for individuals to update or correct their personal data Maintain and implement procedures to provide for and respond to requests for information		

1798.110 This section addresses the right to request disclosure of: ● categories of personal information collected about consumers; ● categories of sources from which personal information is collected; ● business or commercial purposes for collection or sale of personal information; ● categories of third parties with whom personal information is shared; and ● specific pieces of personal information collected about a consumer. The section also clarifies that personal information need not	**Maintain and implement procedures to provide for and respond to requests for information** This privacy management activity addresses the primary processes and procedures needed to ensure businesses can respond to requests in a timely and appropriate manner. **Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for required information to be provided to consumers about collection and use of their personal information. **Integrate data privacy into records retention practices** This privacy management activity helps the organization embed data privacy into the records retention schedule to ensure the proper storage of personal information.	Protocol or procedure for responding to disclosure requests Disclosure request form Template letters for responding to requests Disclosure request log Procedures for responding to customer requests Customer service mailbox Data privacy notice Records retention schedule Data privacy policy	Documentation that workflows for request demonstrate that procedures are being followed Random audit of files that demonstrates that templates are used in communications with requestors Documentation that customer service mailbox is tested to verify it is monitored and responded to Log tracking requests validates that timelines for responses are met Copy of the information notice provided to consumers Documentation showing that privacy notice is aligned to legal requirements Audit results examining that the retention schedule was followed Data privacy policy language prohibits re-

be 1) retained if collected for single, one-time transactions if the information is not retained in the ordinary course of business or 2) reidentified, if the information is not maintained in a manner that would be considered personal information. Therefore, organizations need not retain information or re-identify information in order to respond to requests.	**Maintain policies/procedures for secondary uses of personal data** This privacy management activity addresses having policies and procedures that define how to handle situations when the organization wishes to use personal data beyond the primary purpose. **Additional privacy management activities that will help ensure policies and procedures are in place to respond to DSAR requests:** Maintain and implement procedures to provide for and respond to requests for access to personal data Maintain and implement procedures to provide for and respond to requests to opt-out of, restrict or object to processing Maintain and implement procedures to provide for and respond to requests and/or provide a mechanism for		identification of de-identified data

	individuals to update or correct their personal data Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data		
1798.115 This section addresses the right to request, from businesses that sell or disclose personal information for business purposes, disclosure of categories of personal information that the business sold or disclosed and the categories of third parties to whom those categories of personal information were sold or disclosed in the preceding 12 months. Third parties cannot sell personal information that was sold to them from a business unless:	**Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for required information to be provided to consumers about sale of their personal information. **Maintain and implement procedures to provide for and respond to requests for information** This privacy management activity addresses the primary processes and procedures needed to ensure businesses can respond to requests in a timely and appropriate manner. **Maintain and implement procedures to provide for and respond to requests to**	Data privacy notice Opt-out request form Disclosure request form Procedures for responding to customer requests Template letters for responding to requests Request log Customer service mailbox	Copy of the information notice provided to consumers Documentation showing that privacy notice is aligned to legal requirements Documentation that workflows for request demonstrate that procedures are being followed Random audit of files that demonstrates that templates are used in communications with requestors Documentation that customer service mailbox is tested to verify it is monitored and responded to Log tracking requests validates that timelines for responses are met

● notice is given to consumers; and ● they have an opportunity to opt out.	**opt-out of, restrict or object to processing** This privacy management activity addresses the primary processes and procedures needed to ensure consumers can opt-out of sale of their personal information upon request, in a timely and effective manner. **Additional privacy management activities that will help ensure policies and procedures are in place to respond to DSAR requests:** Maintain and implement procedures to provide for and respond to requests for access to personal data Maintain and implement procedures to provide for and respond to requests and/or provide a mechanism for individuals to update or correct their personal data Maintain and implement procedures to provide for and respond to requests for data portability		Audit results that procedures are being followed

	Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data **Additional privacy management activities that if in place will help address the requirement to provide notice and opt-out opportunities where data was received from a third party** Maintain and implement policies/procedures for permissible collection and use of children and minors' personal data Maintain policies/procedures for collection and use of sensitive personal data (including biometric data) Integrate data privacy into use of cookies and tracking mechanisms Integrate data privacy into direct marketing practices Integrate data privacy into email marketing practices		

	Integrate data privacy into telemarketing practices Integrate data privacy into digital advertising practices (e.g. online, mobile) Integrate data privacy into the organization's use of social media Integrate data privacy into use of CCTV/video surveillance Integrate data privacy into use of geo-location (tracking and or location) devices Integrate data privacy into research practices (e.g. scientific and historical research)		
1798.120 This section addresses: ● consumers' right to opt out of sales of personal information; and ● prohibitions on selling minors'	**Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for required information to be provided to consumers about	Data privacy notice Parental consent notice and forms Procedure for verifying parental consent	Documentation showing that privacy notice is aligned to legal requirements Details on delivery and timing of notice

personal information without parental or guardian consent for those under 13, or without opt-in express authorization for 13-15 year olds.	sale of their personal information. **Maintain and implement policies/procedures for permissible collection and use of children and minors' personal data** This privacy management activity ensures certain policies and procedures are in place to ensure consent is given or authorized by a parent or guardian for sale of a minors' personal information. **Maintain policies and procedures for obtaining valid consent** This privacy management activity addresses the requirement to ensure parents or guardians have affirmatively authorized sale of minor consumers' personal information.	Technical solutions for obtaining verifiable parental consent Policy or procedure for responding to requests to opt out of sale of information Procedures for responding to customer requests and preferences Customer or user portal to update data Customer service mailbox	Copy of the information notice provided to consumers Email confirmations Completed consent forms/evidence of opt-in consent Call-center recordings Audit results that protocols are being followed Customer service mailbox is tested to verify the mailbox is monitored and responded to Test results for portal functionality
1798.125 This section: ● contains prohibitions against	**Maintain a data privacy notice** This privacy management activity ensures policies and	Data privacy notice Procedure for verifying consumers' prior, opt-in	Copy of the information notice provided to consumers

discrimination against consumers for opting out of sales of their personal information; and ● addresses when financial incentives may be used.	procedures are in place for required information to be provided to consumers about financial incentives offered as compensation for collection, sale or deletion of personal information. **Maintain policies and procedures for obtaining valid consent** This privacy management activity addresses the requirement to ensure consumers have provided consent for financial incentive programs.	consent for financial incentive programs Consent forms	Documentation showing that privacy notice is aligned to legal requirements Completed consent forms/evidence of opt-in consent
1798.130 This section has obligations to implement mechanisms to comply with consumer requests received including: ● Two or more methods for consumers to submit requests, including a toll-free telephone number;	**Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for required information to be provided to consumers about financial incentives offered as compensation for collection, sale or deletion of personal information.	Data privacy notice Policy or procedure for responding to requests to opt out of sale of information Protocol or procedure for responding to access requests Access request form Template letters for responding to requests Access request log	Copy of the information notice provided to consumers Documentation showing that privacy notice is aligned to legal requirements Documentation that workflows for request demonstrate that procedures are being followed Random audit of files that demonstrates that templates

• Disclosure of requested information, free of charge, within 45 days of request receipt; • Authentication of the consumer; • Disclosure of privacy notices containing descriptions of consumers' rights; • Provision of an email address for submitting requests if the business operates exclusively online and has a direct relationship with consumers from whom it collects PI; • Ensuring responsible employees are informed of how consumers can exercise their right to opt out of sale of their personal information; and • the option to require submission of	**Maintain and implement procedures to provide for and respond to requests to opt-out of, restrict or object to processing** This privacy management activity addresses the primary processes and procedures needed to ensure records of personal data are used in line with any restrictions on uses by business and any third parties. **Maintain and implement procedures to provide for and respond to requests for access to personal data** This privacy management activity addresses the primary processes and procedures needed to ensure businesses can respond to access requests in a timely and appropriate manner.	Procedures for responding to customer requests Customer service mailbox Policy or procedure for responding to requests for information Procedures for responding to customer requests and preferences Protocol or procedure for responding to deletion request Personal data inventory Data classification scheme Training and awareness materials Data privacy policy Procedures for responding to customer requests and preferences	are used in communications with requestors Documentation that customer service mailbox is tested to verify it is monitored and responded to Log tracking requests validates that timelines for responses are met Audit results that protocols are being followed Reviews of customer service interactions validating that guidelines are being followed Personal data inventory identifies CCPA relevant data and categories Data classification scheme categorizes data in a way that aligns with CCPA categories Documentation showing the content and delivery of a training and awareness program

requests through accounts consumers maintain with the business. This section goes on to provide that information collected for the purpose of verifying the request shall only be used for that purpose.	**Maintain and implement procedures to provide for and respond to requests for information** This privacy management activity addresses the primary processes and procedures needed to ensure businesses can respond to requests in a timely and appropriate manner. **Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data** This privacy management activity addresses the primary processes and procedures needed to ensure personal information are deleted upon request, where appropriate, in a timely and effective manner. **Maintain and implement procedures to provide for**		Policy language restricts the use of requestor personal information to solely responding to requests Audit results demonstrate that protocols are being followed and personal information is not used other than for responding to requests

	and respond to requests and/or provide a mechanism for individuals to update or correct their personal data This privacy management activity addresses the primary processes and procedures needed to ensure personal information can be updated. **Maintain an inventory of personal data and/or other processing activities** This privacy management activity will help identify where data is stored in order to facilitate requests and what categories of data and third parties are involved in processing activities. **Classify personal data holdings by type (e.g., sensitive, confidential, public)** This privacy management activity aids organizations in establishing a classification scheme that identifies the categories of personal		

	information and details of data ownership and providence. **Conduct privacy training reflecting job specific content** This privacy management activity addresses the need to provide awareness and training of staff involved in processing consumer requests around how individuals can exercise their CCPA rights and their right not to be discriminated against for exercising such rights. **Maintain policies/procedures for secondary uses of personal data** This privacy management activity addresses having policies and procedures that define how to handle situations when the organization wishes to use personal data beyond the primary purpose.		
1798.135 This section addresses obligations to: ● provide consumers with a Do Not Sell	**Maintain a data privacy notice** This privacy management activity ensures policies and procedures are in place for	Data privacy notice Training and awareness materials	Copy of the information notice provided to consumers

My Information link; ● provide consumers with an information notice; ● ensure responsible employees are informed of how consumers can exercise their right to opt out of sale of their personal information; ● ensure opt-out requests are honored. The section additionally provides that: ● businesses cannot require consumers to create accounts in order to direct the business not to sell their personal information; ● requests for re-authorization to sell personal information may not be made for 12 months from the request to opt-out;	required information to be provided to consumers about sale of their personal information. **Provide notice by means of on-location signage, posters** This privacy management activity ensures required information is provided to consumers in brick and mortar relationships. **Conduct privacy training reflecting job specific content** This privacy management activity addresses the need to businesses to provide awareness-training and training of staff involved in processing consumer requests and implementing such activities would produce documentation that could serve as evidence of compliance with this requirement. **Maintain policies/procedures for secondary uses of personal data**	Policy or procedure for responding to requests to restrict processing of information Policy or procedure for responding to requests to opt out of sale of information Procedures for responding to customer requests and preferences Customer or user portal to update data Customer service mailbox Data privacy policy Procedures for responding to customer requests and preferences Customer Relationship Management (CRM) System	Documentation showing that privacy notice is aligned to legal requirements Documentation showing the physical locations of privacy notice posters Test results for the “Do Not Sell” link functionality Documentation showing the content and delivery of a training and awareness program Reviews of customer service interactions validating that guidelines are being followed Customer service mailbox is tested to verify the mailbox is monitored and responded to Test results for portal functionality Test results for the “Do Not Sell” link functionality Policy language restricts the use of requestor personal

● information collected for the purpose of submitting the request shall only be used for that purpose.	This privacy management activity addresses having policies and procedures that define how to handle situations when the organization wishes to use personal data beyond the primary purpose. **Maintain and implement policies/procedures for obtaining valid consent** This privacy management activity addresses the requirement to ensure consumers have provided consent for sales of their personal information. **Additional privacy management activities that if in place will help address the requirement to not sell personal information where the opt-out is exercised.** Maintain and implement policies/procedures for permissible collection and use of children and minors' personal data Maintain policies/procedures for collection and use of		information to solely responding to requests Audit results demonstrate that protocols are being followed and personal information is not used other than for responding to requests CRM notes showing time-stamped entries related to Do Not Sell requests and notes about when requests to reauthorize sales may be made..

	sensitive personal data (including biometric data) Integrate data privacy into use of cookies and tracking mechanisms Integrate data privacy into direct marketing practices Integrate data privacy into email marketing practices Integrate data privacy into telemarketing practices Integrate data privacy into digital advertising practices (e.g. online, mobile) Integrate data privacy into the organization's use of social media Integrate data privacy into use of CCTV/video surveillance Integrate data privacy into use of geo-location (tracking and or location) devices Integrate data privacy into research practices (e.g.		

	scientific and historical research)		
1798.140 This section defines common terms in the Act. Many terms will be relevant for determining whether the CCPA applies to the organization. Additional text in some of the definitions contain qualifiers or exceptions, to which certain actions must be taken to qualify, such as requiring privacy notice to consumers in the case of mergers and acquisitions in order to fall under an exception to what is considered a "sale" of personal information. Or particular contract requirements in order to fall within an exception to who is a "third party".	**Maintain a data privacy policy** This privacy management activity helps the organization create and maintain an organization-level privacy policy to provide guidance to employees and ensure any processing complies with the CCPA. **Maintain a data privacy notice** This privacy management activity ensures that required information is provided to consumers when third party recipients intend to change how personal information is used or shared. **Provide notice by means of on-location signage, posters** This privacy management activity ensures required information is provided to consumers in brick and mortar relationships.	Data privacy policy Data privacy notice Data privacy and security requirements for third parties Procurement policy Template contract language for privacy requirements Procedure/workflow for executing contracts	Audit of processing activities demonstrating that privacy protocols were followed Communications with legal department or outside counsel regarding application of CCPA to operations Copy of the information notice provided to consumers Documentation showing that privacy notice is aligned to legal requirements Documentation showing the physical locations of privacy notice posters Contracts with third parties creating prohibitions on sales of personal information, retaining, using or disclosing personal information for any purpose other than the services contracted for, and retaining,

	Maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates) This privacy management activity helps the organization determine what data protection requirements are needed for contracts with third-parties who receive the personal data from the organization. **Maintain procedures to execute contracts or agreements with all processors** This privacy management activity addresses steps taken to ensure written or electronic contracts are in place with processors.		using or disclosing the information outside of the direct business relationship Certifications from service providers that they understand restrictions on the use and disclosure of personal information
1798.145 This section addresses limitations on the application of the Act, creating exceptions from the CCPA (information or entities covered under other	**Maintain a data privacy policy** This privacy management activity ensures policies and procedures are in place to address how the organization will collect, use and process data in accordance with CCPA.	Data privacy policy Protocol or procedure for responding to disclosure requests Disclosure request form	Documentation that policies have been reviewed and updated where necessary to align with CCPA exceptions Documentation that employees have received and understood information

laws, such as FCRA, GLBA, HIPAA, etc.) and activities that are not impacted by the CCPA rights. The section also addresses operational aspects of responding to requests, including extensions on the time frame for responses, and charging fees for excessive or unfounded requests. The section clarifies that entities are not expected to collect personal information other than normally collected in the course of business merely for the purpose of responding to a request. Finally, the section provides that organizations remain liable for the violations of service providers, where the organization has knowledge or a	**Maintain and implement procedures to provide for and respond to requests to opt-out of, restrict or object to processing** This privacy management activity addresses the primary processes and procedures needed to ensure compliance with consumers' requests. **Maintain and implement procedures to provide for and respond to requests for information** This privacy management activity addresses the primary processes and procedures needed to ensure businesses can respond to requests in a timely and appropriate manner. **Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data** This privacy management activity addresses the primary processes and procedures	Template letters for responding to requests Disclosure request log Procedures for responding to customer requests Customer service mailbox Policy or procedure for responding to requests to opt out of sale of information Procedures for responding to customer requests and preferences Protocol or procedure for responding to deletion request Due diligence checklists Vendor self-assessment forms	handling policies, training and awareness programs Documentation that workflows for requests demonstrate that procedures are being followed Random audit of files that demonstrates that templates are used in communications with requestors Documentation that customer service mailbox is tested to verify it is monitored and responded to Log tracking requests validates that timelines for responses are met Audit results that protocols are being followed Completed due diligence checklists Completed vendor self-assessments

reason to believe that the service provider is using personal information in violation of restrictions.	needed to ensure personal information is deleted upon request, where appropriate, in a timely and effective manner. **Maintain and implement procedures to provide for and respond to requests and/or provide a mechanism for individuals to update or correct their personal data** This privacy management activity addresses the primary processes and procedures needed to ensure personal information can be updated. **Conduct due diligence around the data privacy and security posture of potential vendors/processors** This privacy management activity addresses the need to ensure that service providers are not using personal information in a manner that violates the contract. **Maintain policies/procedures for the de-identification of personal data**		

	This privacy management activity ensures that policies address the fact that re-identification of personal information is not necessary to respond to CCPA requests		
1798.150 This section provides consumers with the right to institute a civil action for relief or damages resulting from a breach of their non-encrypted and non-redacted personal information. The breach must result from a violation of the duty to implement and maintain reasonable security procedures and practices, appropriate to the nature of the information.	**Maintain a data privacy incident/breach response plan** This privacy management activity ensures a plan is in place to respond when violations or breaches of personal information are discovered. **Conduct periodic testing of data privacy incident/breach plan** This privacy management activity ensures that the plan to respond to breaches of personal information is tested to determine its efficacy and whether enhancements are required.	Data breach response plan Data breach notification protocol Data breach metrics Data breach response plan testing	Documentation of breach analysis showing whether non-encrypted, non-redacted personal information was implicated Test results showing that the breach response plan can be executed effectively
1798.155 This section provides for the imposition of fines up to $7,500 for	**Obtain regulator approval for data processing (where prior approval is required)**	Regulator approval for data processing Ad hoc communication in response to privacy issue	Copies of the communications Formal response from the Attorney General

each violation of the Act. This section also allows for businesses to seek the opinion of the Attorney General for compliance guidance	This privacy management activity addresses seeking validation from regulators in advance of processing activities.	Consultation with the Attorney General	

1798.160

This section provides for a Consumer Privacy Fund to be created within the State Treasury to offset costs incurred by the courts or the Attorney General in connection with actions brought to enforce the Act. There are no accountability obligations formed by this section.

1798.175

This section establishes that the provisions of the Act are not limited to information collected electronically or over the internet but apply to collection and sale of all consumer personal information collected by a business. There are no accountability obligations formed by this section.

1798.180

This section establishes that the Act supersedes and pre-empts all rules, regulations, codes, ordinances and other laws adopted by cities, counties, municipalities or local agencies in the State. There are no accountability obligations formed by this section.

1798.185

This section provides for public participation in the Attorney General adopting regulations to further the purposes of the Act by its effective date of January 1, 2020. There are no accountability obligations formed by this section.

1798.190

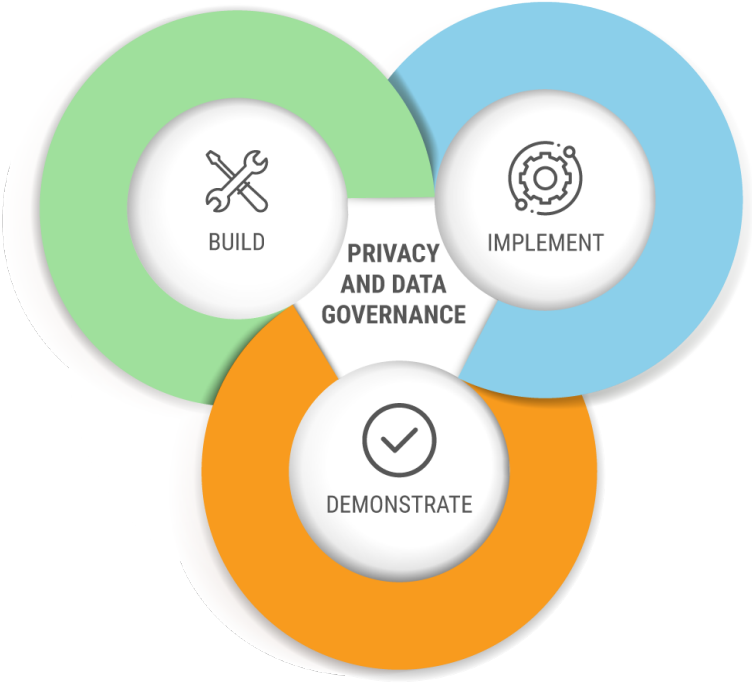
This section provides for the court to disregard intermediate steps taken, or transactions conducted, by businesses to avoid the scope of the Act. There are no accountability obligations formed by this section.

1798.192 This section states that any contract or agreement provisions that waive or limit consumers' rights under the act shall be deemed contrary to public policy, void and unenforceable. There are no accountability obligations formed by this section.
1798.194 This section provides for liberal interpretation of the Act. There are no accountability obligations formed by this section.
1798.196 The Act is not applicable if pre-empted by, or in conflict with, federal law or the California Constitution. There are no accountability obligations formed by this section.
1798.198 The Act shall be operative January 1, 2020.

PART 2

An Accountability Approach to Demonstrating Compliance with the GDPR and CCPA

TrustArc Privacy Frameworks



Overview

The General Data Protection Regulation ("GDPR") integrates accountability as a principle in Article 5(2) which requires organizations to demonstrate compliance with the principles of the GDPR. Article 24 sets out how organizations can do this by requiring the implementation of appropriate technical and organizational measures to ensure that organizations **can** demonstrate that the processing of personal data is performed in accordance with the GDPR. While the CCPA does not legally require the demonstration of compliance, section 1798.155 provides a safe harbor from civil actions for non-compliance where the business is able to cure a violation within 30 days of being provided notice of the violation. Being able to quickly address violations and demonstrate compliance with the CCPA has become a compelling event for organizations to invest in privacy programs. For multinational organizations, the most effective, efficient, and scalable approach is to implement and maintain one consistent privacy management program that maps to multiple laws. The below chart identifies common privacy management activities between both the GDPR and CCPA mapped to the TrustArc Privacy and Data Governance Framework. GDPR articles are only included for those privacy management activities that support CCPA compliance to demonstrate the overlap between how a framework approach to privacy management can help an organization achieve both GDPR and CCPA compliance; to achieve full GDPR compliance, additional privacy management activities are required.

The TrustArc Privacy and Data Governance Framework consists of a set of operational controls that is aligned with key privacy laws, regulatory frameworks, and requirements for ethics and compliance programs and information governance programs, such as the OECD Privacy Guidelines, the APEC Privacy Framework, the GDPR, the U.S. Health Insurance Portability and Accountability Act ("HIPAA"), and ISO 27001 International Standard for Information Security Management Systems. The TrustArc Privacy and Data Governance Framework supports all 3 phases, BUILD, IMPLEMENT, and DEMONSTRATE, of program management on an ongoing basis. The privacy management activities ("technical and organizational measures") identified below under the three pillars of Build, Implement, and Demonstrate emerged from the privacy management categories enumerated in the Nymity Privacy Management Accountability Framework and serve, not as a checklist of activities that must be completed, but as a menu for accountability that can be adapted to any organizations. Taking a Framework approach enables organizations to design and/or engineer effective privacy and data governance controls into organizational processes, products and technologies, and maintain, monitor and enhance those controls throughout the lifecycle for the product, process or technology.

Before the GDPR and the CCPA, there were already 100s of privacy and data protection laws and regulations and there will be many more new privacy laws in the months and years to come. Privacy legislation will always be subject to change, no

matter where an organization is located and in how many countries it operates. An accountability approach to compliance is the most pragmatic, scalable, and proven method for supporting compliance with multiple laws. No two organizations' accountability requirements are the same, and thus the TrustArc Privacy and Data Governance Framework provides the flexibility necessary for planning, scaling, and communicating privacy management and is ideally suited to address the risk-based approach inherent in the GDPR. The appropriate technical or organizational measures to put in place are determined based on the organization's legal and regulatory compliance requirements, risk profile, business objectives, and the context of data processing (type of data processed, nature of processing, purpose for processing).

This Part is designed to support the ability of the Privacy Office in implementing an accountability approach to compliance with the CCPA and GDPR. An accountability approach to demonstrating compliance with laws means organizations implement and maintain appropriate privacy management activities (technical and organizational measures) that create a capacity to comply over time and produce documentation and reports that provide evidence of compliance. This Part not only identifies those technical and organizational measures that are required to demonstrate legal compliance, but also those privacy management activities that will help organizations be able to tell the story behind their privacy program and to be able to demonstrate they have an ongoing *capacity to comply* with legal requirements on an ongoing basis. Not only the policies and procedures need to be in place, but also the review mechanisms and the understanding of the organizations' data processing operations is relevant.

For example: organizations dealing with CCPA can implement procedures to respond to requests for information from Californian residents, as is required by article 1798.110 CCPA. However, when looking at said article, consumers can request disclosure of the categories of personal information collection, as well as categories of sources from which personal information is collected and more. To be accountable, organizations will therefore also need to understand their own data processing operations and have a good overview of the data that are processed and the reasons why this is done. The below privacy management activities can be used by organizations to determine their unique organizational Framework for compliance, which will support the compliance obligations by producing documentation to help demonstrate compliance:

Privacy and Data Governance Pillar	Technical and Organizational Measures	GDPR Article Reference	CCPA Provision Reference
Privacy Management Category 1. Maintain Governance Structure			
Build	Assign responsibility for data privacy to an individual (e.g. Privacy Officer, General Counsel, CPO, CISO, EU Representative)		
	Engage senior management in data privacy (e.g. at the Board of Directors, Executive Committee)		
	Appoint a Data Protection Officer (DPO) in an independent oversight role		
	Assign responsibility for data privacy throughout the organization (e.g. Privacy Network)		
	Maintain roles and responsibilities for individuals responsible for data privacy (e.g. Job descriptions)		
	Conduct regular communication between the privacy office, privacy network and others		

	responsible/accountable for data privacy		
	Engage stakeholders throughout the organization on data privacy matters (e.g., information security, marketing, etc.)		
	Conduct an Enterprise Privacy Risk Assessment		
	Integrate data privacy into business risk assessments/reporting		
	Maintain a privacy strategy		
	Maintain a privacy program charter/mission statement		
	Require employees to acknowledge and agree to adhere to the data privacy policies		
Demonstrate	Report to internal stakeholders on the status of privacy management (e.g. board of directors, management)		
	Report to external stakeholders on the status of privacy management (e.g., regulators, third–parties, clients)		
Privacy Management Category 2. Maintain Personal Data Inventory and Data Transfer Mechanism			

Build	Maintain an inventory of personal data and/or processing activities	30	1798.130
	Classify personal data by type (e.g. sensitive, confidential, public)	30	1798.130
	Maintain documentation of data flows (e.g. between systems, between processes, between countries)		
Implement	Maintain documentation of the transfer mechanism used for cross-border data flows (e.g., model clauses, BCRs, Regulator approvals)		
	Use contracts as a data transfer mechanism (e.g., Standard Contractual Clauses)		
	Use adequacy or one of the derogations (e.g. consent, performance of a contract, public interest) as a data transfer mechanism		
Demonstrate	Obtain Regulator approval for data processing (where prior approval is required)	27, 31, 37, 39	1798.155

	Register databases with regulators (where registration is required)	27, 31, 37, 39	Under AB 1202, *An Act establishing Data Broker Registration*, data brokers must register annually with the Attorney General
	Use Binding Corporate Rules as a data transfer mechanism		
	Use APEC Cross Border Privacy Rules as a data transfer mechanism		
	Use Regulator approval as a data transfer mechanism		
	Use the Privacy Shield as a data transfer mechanism		
Privacy Management Category 3. Maintain Internal Data Privacy Policy			
Build	Maintain a data privacy policy	1, 2, 3, 4, 23, 24, 91	1798.140, 1798.145
	Maintain an employee data privacy policy		
Implement	Document legal basis for processing personal data		
Demonstrate	Integrate ethics into data processing (Codes of Conduct, policies and other measures)		
	Maintain an organizational code of conduct that includes privacy		

Privacy Management Category 4. Embed Data Privacy Into Operations			
Build	Maintain policies/procedures to review processing conducted wholly or partially by automated means		
Implement	Maintain policies/procedures for collection and use of sensitive personal data (including biometric data)	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Maintain and implement policies/procedures for permissible collection and use of children and minors' personal data	5, 6, 8, 9, 10, 29	1798.115(d), 1798.120(c), 1798.135(a)(4)
	Maintain policies/procedures for maintaining data quality		
	Maintain policies/procedures for the de–identification of personal data	5, 25, 89	1798.145(k)
	Maintain policies/procedures for secondary uses of personal data	5, 6, 11	1798.100(e)(2), 1798.110(d)(2), 1798.130(a)(7), 1798.135(a)(6), 1798.140(t)
	Maintain and implement policies/procedures for obtaining valid consent	7, 8, 22	1798.120(d), 1798.125(b)(3), 1798.135(a) & (c)

	Maintain policies/procedures for secure destruction of personal data		
	Integrate data privacy into use of cookies and tracking mechanisms	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into records retention practices	5	1798.100(e)(1), 1798.110(d)(1)
	Integrate data privacy into direct marketing practices	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into e–mail marketing practices	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into telemarketing practices	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into digital advertising practices (e.g., online, mobile)	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into hiring practices		
	Integrate data privacy into the organization's use of social media practices	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into Bring Your Own Device (BYOD) policies/procedures		
	Integrate data privacy into health & safety practices		

	Integrate data privacy into interactions with works councils		
	Integrate data privacy into practices for monitoring employees		
	Integrate data privacy into use of CCTV/video surveillance	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into use of geo–location (tracking and or location) devices	5, 6, 9, 10, 29	1798.115(d), 1798.135(a)(4)
	Integrate data privacy into delegate access to employees' company e–mail accounts (e.g. vacation, LOA, termination)		
	Integrate data privacy into e–discovery practices		
	Integrate data privacy into conducting internal investigations		
	Integrate data privacy into practices for disclosure to and for law enforcement purposes		
	Integrate data privacy into research practices (e.g., scientific and historical research)	5, 6, 9, 10, 29, 89	1798.115(d), 1798.135(a)(4), 1798.140(s)

Privacy Management Category 5. Maintain Training and Awareness Program			
Build	Conduct privacy training		
	Conduct privacy training reflecting job specific content	39	1798.130(a)(6) 1798.135(a)(3)
	Conduct regular refresher training		
	Incorporate data privacy into operational training (e.g. HR, marketing, call center)		
	Deliver training/awareness in response to timely issues/topics		
	Deliver a privacy newsletter, or incorporate privacy into existing corporate communications		
	Provide a repository of privacy information, e.g. an internal data privacy intranet		
	Maintain privacy awareness material (e.g. posters and videos)		
	Conduct privacy awareness events (e.g. an annual data privacy day/week)		

	Enforce the Requirement to Complete Privacy Training		
	Provide ongoing education and training for the Privacy Office and/or DPOs		
	Maintain qualifications for individuals responsible for data privacy, including certifications		
Demonstrate	Measure participation in data privacy training activities (e.g. numbers of participants, scoring)		
Privacy Management Category 6. Manage Information Security Risk			
Build	Maintain an acceptable use of information resources policy		
Implement	Integrate data privacy risk into security risk assessments		
	Integrate data privacy into an information security policy		
	Maintain technical security measures (e.g. intrusion detection, firewalls, monitoring)		
	Maintain measures to encrypt personal data		
	Maintain procedures to restrict access to personal data (e.g.		

	role–based access, segregation of duties)		
	Integrate data privacy into a corporate security policy (protection of physical premises and hard assets)		
	Maintain human resource security measures (e.g. pre–screening, performance appraisals)		
	Maintain backup and business continuity plans		
	Maintain a data–loss prevention strategy		
Demonstrate	Conduct regular testing of data security posture		
	Maintain a security certification (e.g. ISO)		
Privacy Management Category 7. Manage Third-Party Risk			
Build	Maintain data privacy requirements for third parties (e.g. clients, vendors, processors, affiliates)	28	1798.105(c), 1798.140(w)
	Conduct due diligence on third party data sources		
	Maintain a vendor data privacy risk assessment process		

	Maintain a policy governing use of cloud providers		
	Maintain procedures to address instances of non–compliance with contracts and agreements		
Implement	Maintain procedures to execute contracts or agreements with all processors	26, 28	1798.105(c), 1798.140(w)
	Conduct due diligence around the data privacy and security posture of potential vendors/processors	28	1798.145(j)
	Review long–term contracts for new or evolving data privacy risks		
Demonstrate	Conduct due diligence around the data privacy and security posture of existing vendors/processors		
Privacy Management Category 8. Maintain Notices			
Implement	Maintain a data privacy notice	13, 14	1798.100(b), 1798.105(b), 1798.110(c), 1798.115(c), 1798.120(b), 1798.125(b)(2), 1798.130(a)(5), 1798.135(a)(2) & (b), 1798.140(t)

	Provide data privacy notice at all points where personal data is collected		
	Provide notice by means of on–location signage, posters	12	1798.135(a), 1798.140(t)
	Provide notice in marketing communications (e.g. emails, flyers, offers)		
	Provide notice in contracts and terms		
	Maintain scripts for use by employees to explain or provide the data privacy notice		
Demonstrate	Maintain a privacy Seal or Trustmark to increase customer trust		
Privacy Management Category 9. Respond to Requests and Complaints from Individuals			
Build	Maintain procedures to address complaints		
	Maintain and implement procedures to provide for and respond to requests for access to personal data	11, 12, 15, 19, 22, 26	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and	11, 12, 16, 19, 22	This right would be introduced by the

	respond to requests and/or provide a mechanism for individuals to update or correct their personal data		Californians for Consumer Privacy ballot initiative, the *California Privacy Rights and Enforcement Act of 2020*
	Maintain procedures to respond to requests to opt–out of, restrict or object to processing	11, 12, 18, 19, 21, 22	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and respond to requests for information		1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and respond to requests for data portability	20	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data	17, 19	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain Frequently Asked Questions to respond to queries from individuals		
	Investigate root causes of data protection complaints		
Implement	Maintain and implement procedures to provide for and respond to requests for access to personal data	11, 12, 15, 19, 22, 26	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)

	Maintain and implement procedures to provide for and respond to requests and/or provide a mechanism for individuals to update or correct their personal data	11, 12, 16, 19, 22	This right would be introduced by the Californians for Consumer Privacy ballot initiative, the *California Privacy Rights and Enforcement Act of 2020*
	Maintain and implement procedures to provide for and respond to requests to opt–out of, restrict or object to processing	11, 12, 18, 19, 21, 22	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and respond to requests for information		1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and respond to requests for data portability	20	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
	Maintain and implement procedures to provide for and respond to requests to be forgotten or for erasure of data	17, 19	1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.145(i)
Demonstrate	Monitor and report metrics for data privacy complaints (e.g. number, root cause)		
Privacy Management Category 10. Monitor for New Operational Practices			

Build	Integrate Privacy by Design into data processing operations		
	Maintain PIA/DPIA guidelines and templates		
	Conduct PIAs/DPIAs for new programs, systems, processes		
	Conduct PIAs or DPIAs for changes to existing programs, systems, or processes		
	Engage external stakeholders (e.g., individuals, privacy advocates) as part of the PIA/DPIA process		
	Track and address data protection issues identified during PIAs/DPIAs		
Demonstrate	Report PIA/DPIA analysis and results to regulators (where required) and external stakeholders (if appropriate)		
Privacy Management Category 11. Maintain Data Privacy Breach Management Program			
Build	Maintain a data privacy incident/breach response plan	33, 34	1798.150(a)
	Maintain a log to track data privacy incidents/breaches		
	Conduct periodic testing of data privacy incident/breach plan	33, 34	1798.150(a)

	Engage a breach response remediation provider		
	Engage a forensic investigation team		
	Obtain data privacy breach insurance coverage		
Demonstrate	Maintain a breach notification (to affected individuals) and reporting (to regulators, credit agencies, law enforcement) protocol		
	Monitor and Report data privacy incident/breach metrics (e.g. nature of breach, risk, root cause)		
Privacy Management Category 12. Monitor Data Handling Practices			
Demonstrate	Conduct self–assessments of privacy management		
	Conduct Internal Audits of the privacy program (i.e., operational audit of the Privacy Office)		
	Conduct ad–hoc walk-throughs		
	Conduct ad–hoc assessments based on external events, such as complaints/breaches		

	Engage a third–party to conduct audits/assessments		
	Monitor and report privacy management metrics		
	Maintain documentation as evidence to demonstrate compliance and/or accountability		
	Maintain certifications, accreditations, or data protection seals for demonstrating compliance to regulators		
Privacy Management Category 13. Track External Criteria			
Build	Identify ongoing privacy compliance requirements, e.g., law, case law, codes, etc.		
	Maintain subscriptions to compliance reporting service/law firm updates to stay informed of new developments		
	Attend/participate in privacy conferences, industry		

	associations, or think–tank events		
	Record/report on the tracking of new laws, regulations, amendments or other rule sources		
	Seek legal opinions regarding recent developments in law		
	Document decisions around new requirements, including their implementation or any rationale behind decisions not to implement changes		
	Identify and manage conflicts in law		

PART 3

Complying with the California Consumer Privacy Act

Complying with the California Consumer Privacy Act

Complying with a new privacy law is never a matter of ticking some boxes: it requires a real effort throughout the organization. In the end, the risk appetite of the organization and the type and volume of information processed will determine what exactly needs to be done in order to get to a satisfactory level of compliance. In this guide, we will present a number of scenarios that will support you in building and implementing a privacy program that is compliant with the California Consumer Privacy Act (CCPA) and will help you to demonstrate such compliance.

Scenario 1: Meeting Basic Level Compliance

Many organizations doing business in California have not had to worry about privacy issues for a long time, except for possibly posting a privacy notice on their website and keeping track of potential data breaches. With the introduction of CCPA as of January 1, 2020 that has changed. All businesses in California meeting the CCPA applicability requirements will now need to ensure they can deal with individual requests from consumers wanting to understand or restrict how their data is processed. With a limited effort, these organizations will be able to meet the basic CCPA compliance requirements.

Does CCPA Apply to My Organization?

CCPA applies only to businesses operating in the State of California that collect personal information. Furthermore, one of the thresholds in the law need to be met:

- Gross revenues in excess of $25 million;
- Collection of personal information of 50,000 or more consumers, households or devices;
- 50% or more of annual revenues derived from selling consumers' personal information.

In addition, CCPA will apply to those businesses that are owned by California-based companies, meaning they hold a majority share or have a decisive influence over the functioning of the business. Also in case of common branding with a California-based business, the CCPA requirements apply to the joint data processing operations.

What are the Basic Requirements?

Under the CCPA, individuals have been granted multiple information rights related to their individual data. First of all, they are allowed to find out "*the categories and specific pieces of personal information*" a business has collected about them. Where personal

information was collected about them, the individual can ask for the deletion of "*any personal information*". Finally, CCPA allows individuals to request from a business an overview of:

- The categories of personal information it has collected about that consumer.
- The categories of sources from which the personal information is collected.
- The business or commercial purpose for collecting or selling personal information.
- The categories of third parties with whom the business shares personal information.
- The specific pieces of personal information it has collected about that consumer.

All in all, an extensive overview needs to be provided at request, within a deadline of 45 days (with a possible extension of another 45 days). It is hard to see how organisations will be able to comply with a request for access, deletion or information, if they don't have a full understanding of the data that is processed in their business and how data flows through the organization. To this end, for many organizations it will quickly become essential to create a data inventory, identifying for each processing operation which categories of data are processed for which purpose, with whom they are shared (including as a sale) and from which source they are collected. This inventory should also be linked to an overview of databases and systems used, to allow for the fast retrieval of the specific pieces of personal information on an individual upon request.

Of note is that businesses should not only technically be able to deal with these kinds of requests, they should also put in place the appropriate policies and procedures that will help them address the requests once they come in. This is what is called accountability. Part of these policies should be how to ensure the individual making the request is actually who they say they are. The Attorney General will provide further guidance in his regulations as to how the verification process should take place.

Beyond the traditional information rights, the CCPA also provides that if the organization "sells" personal information as defined under CCPA, consumers must be informed that personal information is indeed sold to third parties and offered the possibility to opt-out of the sale of their personal information. Businesses that sell personal information are required to place a *clear and conspicuous* link on their website titled 'Do Not Sell My Personal Information', allowing consumers to easily make an opt-out request. A sale of personal information includes more than just the traditional concept of a sale, where a dataset is transmitted from one company to the other in exchange for money. According to Section 1798.140(t) CCPA, a sale includes the "*selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means*" of personal information to "*another business or a third party for monetary or other valuable consideration*". This

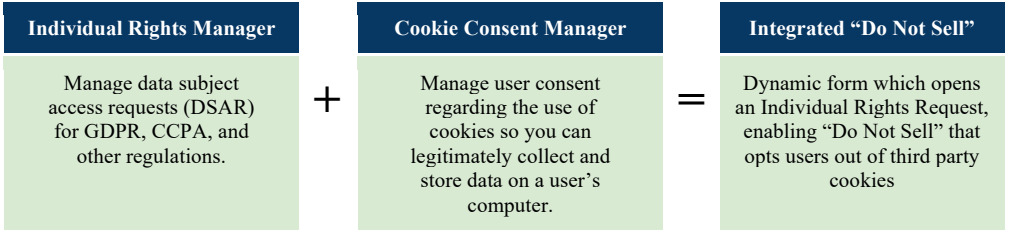
rather broad definition also includes the placement of third party cookies on a website, which in turn means an individual's opt-out should also include the possibility to opt-out of the placement of third party cookies.

As to the question of what constitutes personal information, again CCPA provides for a broader definition that is commonly used under U.S. law. All information that "*identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*" is to be regarded as personal information. Only consumer information "*that is de-identified or aggregate[d]*" does not fall under the scope of CCPA.

In short: if a business collects information that can be reasonably linked to an individual or household, even if it does not know a specific name or address, the individual should be told about this and offered a possibility to opt-out.

How does TrustArc Help?

TrustArc has a comprehensive set of privacy management solutions to help businesses manage all phases of CCPA compliance, comprising the basic tools and information businesses need for a successful privacy program.



- **Individual Rights Management**
  The Individual Rights Management (IRM) module enables businesses to offer consumers a simple mechanism to make requests to access, delete, and opt-out of the sale of personal information, and provides identity verification, automated and integrated workflows, as well as operational reporting to enable businesses to respond timely to there requests they received and to demonstrate compliance.
- **Cookie Consent Management**
  The Cookie Consent Management (CCM) module will help businesses to provide an easy way for customers to opt-out of the use of third-party cookies on their website(s).

  Together, the two modules offer an integrated solution which enables:
  - Dynamic 'Do Not Sell' links, which can be displayed based on geolocation. A customer that is not subject to CCPA will not see the links.
  - Clicking a 'Do Not Sell' link opens a form that will open a ticket in the IRM, allowing the business to keep track of all requests and process them in an organized manner.
  - When a consumer submits the IRM form making a 'Do Not Sell' request, their cookie preferences for the business' website are automatically set to 'opt-out' of all third-party cookies.
- **Operational Templates & Resources**
  Our Operational Templates & Resources is a library of hundreds of sample policies and procedures that will allow businesses to develop the necessary privacy notices and consumer privacy rights handling procedures to comply with CCPA. This includes a whole range of standard notices, that can be tailored to the specific situation of the business, for example providing information on the specific sales of personal information taking place.

Scenario 2: Creating a Demonstrably Compliant Privacy Program

Once the most visual requirements from the CCPA are in place, it is time to take a closer look at compliance. Complying with the 'Do Not Sell' requirement is one, but for full, ongoing compliance more is needed. Under CCPA, consumers also have a right to access their data, to have it deleted (under certain conditions) and to be made aware of all that is happening with their data, also beyond the possible sale.

Where to Start with CCPA Compliance?

Organizations that want to ensure that they can effectively meet all of the transparency and consumer privacy rights requirements unders CCPA on an ongoing basis, whether starting from scratch or not, should start with a gap assessment against current practices. Given that individual rights have existed around the world, including under various U.S. Federal and State laws, many businesses may already have some basic policies and processes in place, for example relating to providing notice on data processing operations via their website, or on dealing with access rights. A gap assessment allows you to find out if the existing policies and procedures are still sufficient, as well as to assess which requirements cannot yet be met.

Once an overview of existing gaps is completed, the project lead will need to decide which steps to prioritize as part of the implementation. Such a decision is best made on the basis of a risk assessment, taking due account of the amount, volume and type of data processed in the organization. When completing this exercise, it would make sense not just to focus on CCPA, but to look at the other privacy requirements under California law as well, especially those related to data security and data breaches.

Apart from providing for policies and procedures to deal with the individual rights of access, deletion and information under CCPA on an ongoing basis, businesses will need to reassess their relationship with third parties as well, whether these are regular business partners or service providers. Contracts need to be reviewed, making sure that they are in line with the CCPA requirements, and risks need to be (re)assessed. Also here, it is likely some sort of prioritization is needed, since no legal team is able to renegotiate every single third party contract at once.

Once the full compliance program is designed and implemented, as a next - and for the time being final - step, the business has an obligation under CCPA to ensure all staff dealing with personal information is trained as well. Training not only has the advantage that your teams will understand their legal requirements, it will also help to raise the overall privacy awareness and privacy standards throughout the organization.

As with all accountability requirements, compliance with CCPA is not a one-off exercise, but requires ongoing attention. Processing operations change, as do the legal requirements and implementation guidelines. Enforcement decisions may also impact the way a business processes personal information. To this end policies and procedures should not only describe what steps to take to get to the desired level of compliance, but also how and how often reviews take place, for example once every two years. Documenting all these steps properly and subsequently acting accordingly will help ensure a business has an ongoing capacity to comply with CCPA and protect the personal information under their control.

How TrustArc Helps

TrustArc has a full suite of solutions that will be able to support organisations subject to CCPA meet their compliance requirements. The modules are well integrated and are able to offer the desired level of support for each organization, from small and midsize company to enterprise level. Each can select the combination of solutions that works best for their specific situation.

Intelligence

The Intelligence stream of our solutions will help an organization assess their operations and the risks involved. The solutions are built on the basis of Privacy Profile, that uses criteria related to business operations to determine whether CCPA is likely to be applicable, provides contextual insights on CCPA and its applicability, and includes a smart CCPA Assessment aligned to specific compliance use cases. The Risk Profile provides insight into third party risk, including for service providers and third parties under CCPA, taking into account the legal requirements and - once available - the implementation guidelines and enforcement criteria.

The Planner and Benchmarks modules help organizations to make the gap assessment at the start of the compliance effort and subsequently to prioritize and monitor implementation efforts at organizational level. A comparison with other organizations within the Benchmarks - based on aggregate data - shows each organizations their progress compared to their peers.

Finally, the various reporting options and dashboards, including an Accountability profile (currently available as Nymity Attestor) allow for various options to report internally, as well as to external stakeholders and regulators, on the level of compliance and progress made.

Knowledge

When building out a compliance program for CCPA, it is important to understand the exact obligations an organisation is subject to, both under the CCPA and other relevant laws in- and outside of California. Nymity Research & Alerts was designed to do exactly that: provide organizations updates on developments in privacy compliance from around the world, including direct access to the full text of all relevant laws and regulations, data subject rights annotations and dashboard widgets that provide immediate access to relevant privacy developments.

Further Knowledge solutions supporting CCPA compliance include Operational Templates, a library of over 900 resources that can be tailored to the specific situation of a business, as well as Legal Summaries and Law Comparisons, that allow for the comparison of legal requirements across multiple jurisdictions.

Operations

The operational compliance with CCPA starts with the integrated Individual Rights Management and Cookie Consent Management solutions, as explained under scenario 1. These solutions will help businesses to provide an easy way for consumers to object against the sale of their data and to opt-out of the use of third-party cookies.

In addition, the Data Inventory Hub enables businesses to complete their data inventory of systems, third parties (including service providers and third parties under CCPA) and data flow mapping, gaining a solid understanding and insight of the data flows in- and transfers outside the organization. This facilitates providing relevant information regarding data collection, use, disclosure, and sale to individuals upon request. It also speeds up the process to find relevant customer information if an exact copy of processed data is requested, especially when the Hub is integrated with an IRM implementation. A data inventory is the foundation of a truly functional privacy program, and when businesses have the Hub - where processes are linked to data elements, service providers, data repositories and systems, and include risk assessment and management - a floundering program becomes functional and integrated.

Hands On Help

For organisations lacking the internal resources to complete the whole CCPA compliance trajectory, TrustArc has a team of consultants available that can support the compliance effort, from gap assessment to the development of internal policies and procedures. For training, we partner with leading privacy e-learning providers, which provide tailored packages that can be used in online learning platforms.

Businesses that have completed their CCPA implementation and are looking for external validation of the work done, can also reach out to TrustArc. We have developed a validation methodology, delivered by our team of expert privacy assurance and certification professionals, to assess your implementation effort and provide tailored feedback and/or confirmation that an organization indeed has an ongoing capacity to comply with CCPA.

Scenario 3: Working Towards Global Privacy Compliance

Before the CCPA and GDPR, there were already hundreds of privacy and data protection laws and regulations and there will be many more new privacy laws in the months and years to come. In the U.S. alone close to two-dozen states have consumer privacy laws under discussion, and all states have some form of data protection requirements focused on special categories of data, certain practices, and/or industries. The same is true for numerous countries in Latin America, South-East Asia, Africa and even Europe. Privacy legislation will always be subject to change, no matter where an organization is located and in how many countries it operates.

Once an organization has completed the implementation of the compliance requirements for a single law, like is described above in scenario 2 dealing with overall CCPA compliance, it is time to look at compliance in multiple jurisdictions at the same time. Of course, it is possible to implement each law individually, and create specific privacy programs for each jurisdiction. However, that is not the most efficient use of time and resources. That is why many multinational or -jurisdictional organizations choose an accountability approach to compliance, because it is the most pragmatic, scalable, and proven method for supporting compliance with multiple laws. An accountability approach to demonstrating compliance with laws means organizations implement and maintain appropriate privacy management activities (technical and organizational measures) that create a capacity to comply over time and produce documentation and reports that provide evidence of compliance. In short: an activities-based privacy program allows organizations to tell the story behind their privacy program and link these activities, and the effectiveness of their implementation, to the specific requirements in the various jurisdictions.

Identifying Global Compliance Needs

When working towards global compliance, organizations will first need to find out which laws they are subject to, both at state, federal and global level. This is largely determined by the location of offices, employees and customers, but could also be influenced by business partners and service providers. To start, it is therefore wise to map out the flows of personal information the organization is dealing with, both internally and externally. Of course, not all locations where data will be processed will have a similar risk to the organization or the data subjects involved in the processing operation. This is step two of creating your privacy profile: where do you consider the risk of your data processing operations is highest? Once these two steps are completed, you will be able to create an overview of relevant locations and identify which are the privacy, data protection and possibly data security laws and regulations that you will have to comply with. The 2019 IAPP/TrustArc Measuring Privacy Operations study shows that 10% of

respondents estimate they need to comply with over 50 laws. For U.S. organizations, this percentage is even higher at 15%. Meeting the requirements of all these laws separately would be virtually impossible, or at least very costly.

Once you have identified the different laws your organization will need to comply with, you can detect the overlap between the various laws. Many of these will have one or more provisions related to individual rights, for example, or related to the notification of data breaches. This means it is probable one policy can deal with the needs of those various laws: the internal procedure on how to respond to an access request will not be different if the request comes from Germany or if it is made in California. In both situations, someone in your organization will need to verify the identity of the requestor, understand what data they are looking for, collect the information relevant to the answer and finally provide the answer to the requestor. The basic policy could explain all these required steps. The differences will mainly relate to the time period that can be used to provide an answer and possibly to what data can and/or should be provided following the request. This however does not need to be part of an organization's Access Request Policy but can also be laid down in additional instructions that are provided to the teams in the various regions.

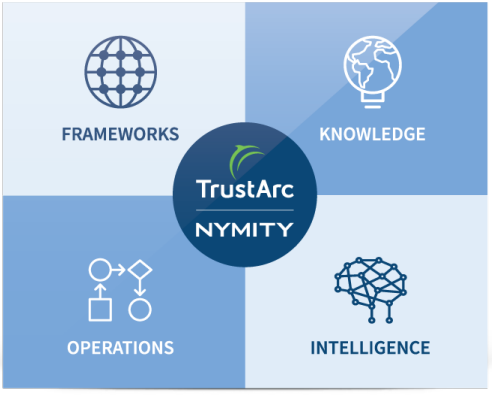
The process identifying the overlap between the laws and regulations an organization needs to comply with will also show the gaps that may still exist in your privacy program to deal with requirements that don't exist under the legislation used to build out your privacy management program. For any gap, the approach would be similar to what was described before under scenario 2: once the gaps are identified, the next step is to develop a prioritized action plan to address the gaps. This may also include the appointment of additional privacy team members, like a Chief Privacy Officer, Data Protection Officer or Privacy Lead, depending on the legal requirements in the jurisdictions you are looking at. Furthermore, any processing activities register, or data inventory, will need to meet the requirements in the various jurisdictions. For this kind of documentation, the laws only provide for minimum requirements. You are free to harmonize your register or inventory in such a way it meets your global needs using a single approach, as long as all the minimum elements are included.

Organizations that have built their privacy program with CCPA in mind will likely be confronted with the need to develop additional policies for data breaches, although it is also possible those were already developed by a security department. Again, there is no need to reinvent the wheel: just like privacy policies and procedures can be repurposed for compliance with other laws, security policies and procedures can be leveraged to comply with certain privacy requirements.

How TrustArc Helps

The software solutions in the TrustArc platform provide a great basis to work towards a globally compliant privacy program. This starts with the Privacy Profile and Risk Profile that are included in our assessment solutions. The Privacy Profile will first help organizations to identify which laws apply to their data processing operations, whereas the Risk Profile subsequently can help to mitigate risks caused by gaps in the privacy program. Other solutions, including Individual Rights Management and Data Inventory Hub have been developed with global compliance needs in mind and allow organizations to monitor and update their compliance efforts on an ongoing basis.

To support organizations in their efforts to manually identify the overlap between laws and regulations, the TrustArc Privacy & Data Governance (P&DG) Framework is mapped to all the hundreds of privacy and data protection laws in the Nymity Research & Alerts database – currently around 850. For each of the provisions of these laws, subscribers to the solution can see in what privacy management category they fall, from 'Embedding Data Privacy into Operations' to 'Maintaining Notices' or 'Responding to Requests and Complaints from Individuals'. This also facilitates the alignment of policies and procedures. In case of gaps, Nymity Operational Templates and Resources provide quick access to relevant sample procedures that can be edited to suit the organization's needs and practices. Nymity Research & Alerts also ensures organizations will stay up to date on their requirements, providing daily updates on developments in the privacy community.



Finally, the reporting options that exist across the TrustArc platform, allow for easy compliance reporting to internal stakeholders, like a Board or an audit department, external partners as well as to regulators and supervisory authorities.

PART 4

Full Text of the California Consumer Privacy Act of 2018

California Civil Code - Division 3 - Part 4 - Title 1.81.5 California Consumer Privacy Act of 2018
https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

1798.100. (a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

1798.105. (a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information

pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the *California Electronic Communications Privacy Act* pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

1798.110. (a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that

consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

1798.115. (a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

1798.120. (a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

1798.125. (a)(1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the business by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision, shall notify consumers of the financial incentives pursuant to Section 1798.130.

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

1798.130. (a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. 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 for information required to be disclosed pursuant to Section 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Section 1798.110 and 1798.115.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business' receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those policies, on its internet website, and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Section 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

1798.135. (a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

1798.140. For purposes of this title:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, 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.

(c) "Business" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "Business purpose" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is

compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided that the personal information is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "Commercial purposes" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or

effecting, directly or indirectly, a commercial transaction. "Commercial purposes" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "Consumer" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) "Designated methods for submitting requests" means a mailing address, email address, internet web page, internet web portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "Device" means any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.

(k) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "Homepage" means the introductory page of an internet website and any internet webpage where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page,

and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.135, including, but not limited to, before downloading the application.

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

(n) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

(o) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the *Family Educational Rights and Privacy Act* (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

(3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information.

(p) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "Processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "Research" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Not be used for any commercial purpose.

(9) Subjected by the business conducting the research to additional security controls that limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (1) “Sell,” “selling,” “sale,” or “sold,” means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s personal information by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not

constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice of that information being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer 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 business provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "Service" or "services" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "Service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for

the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "Third party" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "Unique identifier" or "Unique personal identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a

device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.100, 1798.105, 1798.110 and 1798.115 if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

1798.145. (a) The obligations imposed on businesses by this title shall not restrict a business' ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a

business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the *Health Insurance Portability and Accountability Act of 1996* (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of *Title 15 of the United States Code*, by a furnisher of information, as set forth in Section 1681s-2 of *Title 15 of the United States Code*, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of *Title 15 of the United States Code*, and by a user of a consumer report as set forth in Section 1681b of *Title 15 of the United States Code*.

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the *Fair Credit Reporting Act*, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the *Fair Credit Reporting Act*.

(3) This subdivision shall not apply to Section 1798.150.

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) (1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the *Vehicle Code*, and the vehicle's manufacturer, as defined in Section 672 of the *Vehicle Code*, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of *Title 49 of the United States Code*, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(B) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(h) (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the *Business and Professions Code* and a clinical psychologist as defined in Section 1316.5 of

the *Health and Safety Code*.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

(i) Notwithstanding a business' obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing

the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(l) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

(m) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the *California Constitution*.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.

(2) For purposes of this subdivision:

(A) “Contractor” means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021.

1798.150. (a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented

by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

1798.155. (a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to

subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

1798.160. (a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General's duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

1798.175. This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

1798.180. This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

1798.185. (a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section

1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to Section 1798.120.

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the

administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as follows:

(1) To establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns.

(2) As necessary to further the purposes of this title.

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

1798.190. If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

1798.192. Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

1798.194. This title shall be liberally construed to effectuate its purposes.

1798.196. This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

1798.198. (a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

1798.199. Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

CCPA Accountability Handbook

A Comprehensive Compliance Guide for the California Consumer Privacy Act of 2018

www.trustarc.com