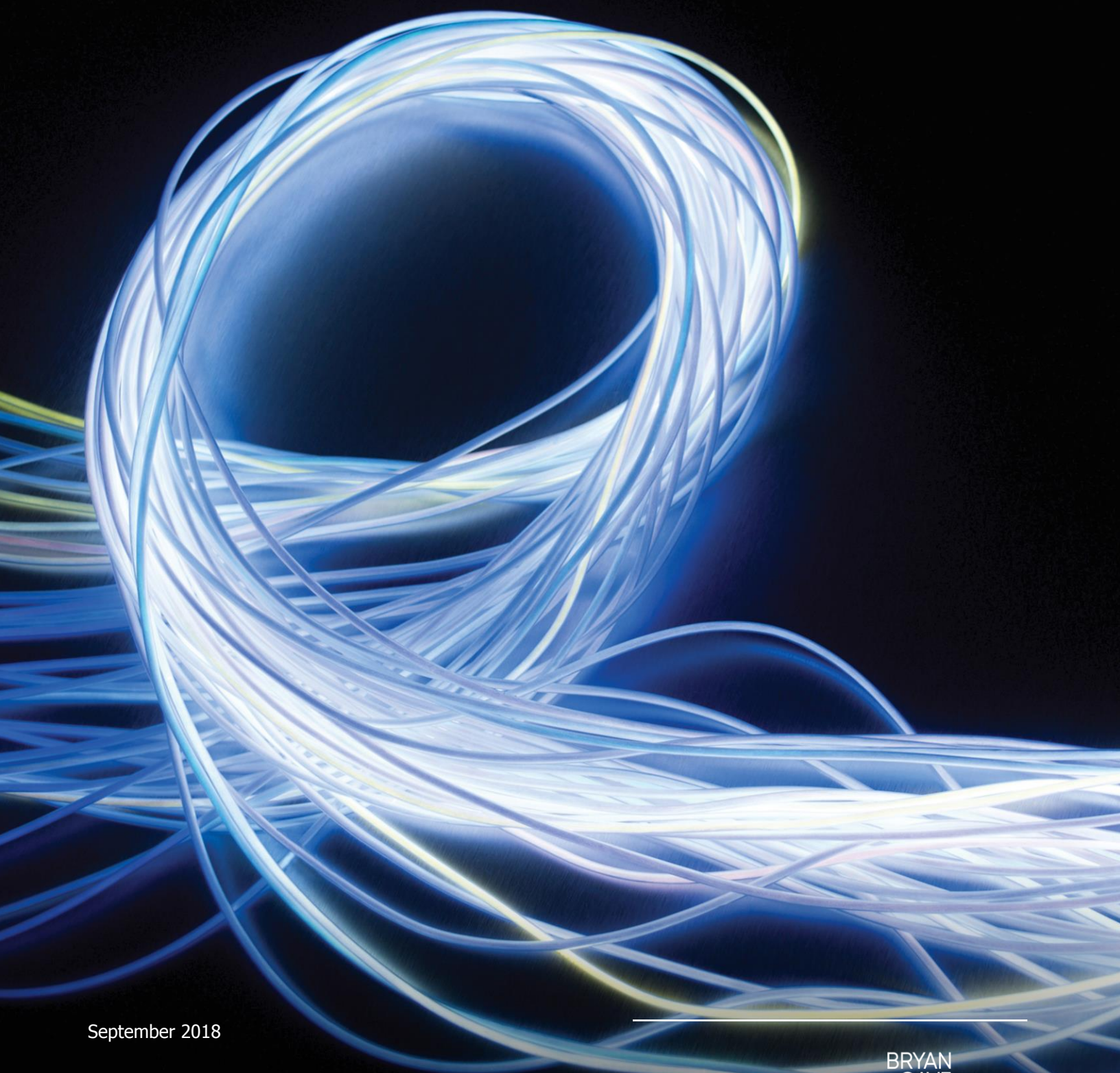


CALIFORNIA CONSUMER PRIVACY
ACT (CCPA)
PRACTICAL GUIDE



September 2018

bcplaw.com

BRYAN
CAVE
LEIGHTON
PAISNER 

Content

Introduction	1
History of the CCPA	1
Proposed vs legislative CCPA	2
Scope of the CCPA.....	3
Summary of Compliance Requirements	4
Privacy notices	5
Right to Access Data.....	7
Right to be Forgotten	8
Right to Opt-Out from Having Information Sold.....	10
Right to Opt-IN to Having Information Sold (Minors)	11
Right to Receive Services on Equal Terms.....	12
Data Security	13
Service Provider Agreements.....	15
Text of the CCPA.....	16
Data privacy and security team	37



David Zetoony

Partner
Chair, Data Privacy and Security Team
T: +1 303 417 8530
david.zetoony@bclplaw.com

INTRODUCTION

As one of the oldest and most recognized data privacy and security practices, we have had the honor of helping dozens of companies set up, and evolve, their data privacy programs over the past decade. That experience has given us unique insight into how companies – from virtually every sector – address new and evolving privacy frameworks.

While the California Consumer Privacy Act is in many respects a “game changer,” it is far from the first “game changer” in the area of data privacy. This guide provides a straight-forward summary of what the Act requires, and, for those companies with developed privacy programs that are already compliant with other United States and European laws, an explanation of the “delta” – i.e., how this law differs from what you already know. My hope is that it is a useful resource both for companies that are new to privacy and for companies that have spent years navigating the twists and turns of this exciting area of law.

Sincerely,

David Zetoony

Bryan Cave Leighton Paisner



HISTORY OF THE CCPA

California Consumer Privacy Act (CCPA) proposed

Activist and San Francisco real estate developer Alastair Mactaggart proposes ballot initiative to change California privacy laws under title California Consumer Privacy Act. The Act is generally opposed by the technology community.

NOV
2017

Facebook withdraws opposition to the CCPA

Following the testimony of Mark Zuckerberg to a joint hearing of the Senate Judiciary and Commerce Committees on the Cambridge Analytica scandal, Facebook withdraws its opposition to the CCPA.

APR
2018

CCPA is placed on the November ballot

Californians for Consumer Privacy announced that it had obtained sufficient signatures to place the CCPA on the November ballot.

MAY
2018

CCPA is rushed to consideration

The California Senate resurrects an inactive proposal on consumer privacy and rushes it to consideration.

JUN 21
2018

Proposal is passed unanimously in the Senate and Assembly

Comments in the legislative history make clear that the bill was intended as a "legislative effort to reach an agreement" in order to avoid the ballot initiative. As a condition for going into force, the legislature required that the ballot initiative be withdrawn. Authors of the legislation recognized that additional amendments may be needed to "correct errors in the drafting of this legislation" and to clarify areas of ambiguity.

JUN 28
2018

CCPA amended

After criticism from consumer groups, business groups, and the Office of the Attorney General the CCPA is amended to clarify how it interacts with federal privacy laws, and strengthen the ability for consumers to bring lawsuits.

SEP
2018



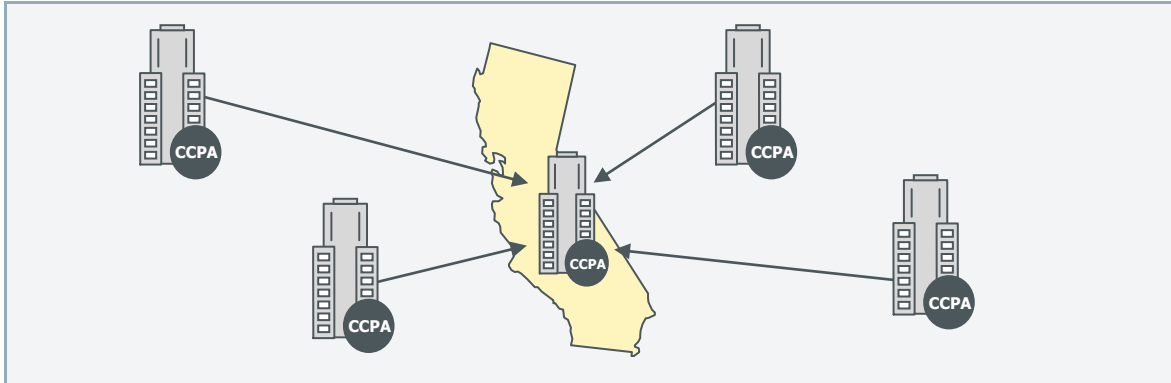
PROPOSED VS LEGISLATIVE CCPA

There are significant differences between the version of the CCPA that was first proposed as a ballot initiative in 2017 and the version of the CCPA that was ultimately passed by the state legislature in 2018. In general, the version passed by the legislature conferred greater data privacy protections, but imposed weaker penalties for non-compliance. The following chart compares the ballot initiative and the final legislative version against the requirements of the European General Data Protection Regulation (“GDPR”) as a common baseline. It is important to note that other California laws overlap with the GDPR as well. For example, while the final version of the CCPA did not include a data breach notification requirement (as noted below), California has a separate, pre-existing, data breach notification law.

	GDPR	CCPA – Ballot Initiative Draft	CCPA - Final Legislative Version
Individual rights	<ul style="list-style-type: none"> ✓ Notices to data subjects ✓ Right to access data ✓ Right to be forgotten ✓ Right to fix errors ✓ Right to object to processing/revoke consent 	<ul style="list-style-type: none"> ✓ Notices to data subjects ✓ Right to access data ✓ Right to opt-out of sale of information ✓ Right to receive services on equal terms 	<ul style="list-style-type: none"> ✓ Notices to data subjects ✓ Right to access data ✓ Right to be forgotten ✓ Right to opt-out of sale of information ✓ Right to receive services on equal terms
Security	<ul style="list-style-type: none"> ✓ Appropriate data security required ✓ Breach notification 	<ul style="list-style-type: none"> ✓ Breach notification 	<ul style="list-style-type: none"> ✓ Appropriate data security required
Service provider	<ul style="list-style-type: none"> ✓ Contractual requirements in service provider agreements 	None	<ul style="list-style-type: none"> ✓ Contractual requirements in service provider agreements
Ability to process data	<ul style="list-style-type: none"> ✓ Permissible Purpose ✓ Data Minimization 	None	None
Data transfers outside EEA	<ul style="list-style-type: none"> ✓ Adequacy measures required for any country determined to have laws that do not parallel EEA 	None	None
Accountability/governance	<ul style="list-style-type: none"> ✓ Internal documentation and record keeping ✓ Designated DPO (if necessary) or other responsible individual 	None	None

SCOPE OF THE CCPA

Like several other European and United States data privacy and security statutes, the CCPA purports to apply extra-territorially – i.e., to companies that may not have offices or employees in California, but that do “business in the State.”



Businesses it does not apply to

Unlike most other data privacy and security statutes, however, the CCPA attempts to carve out small businesses such that it only applies to a business if it falls into one of the following buckets:

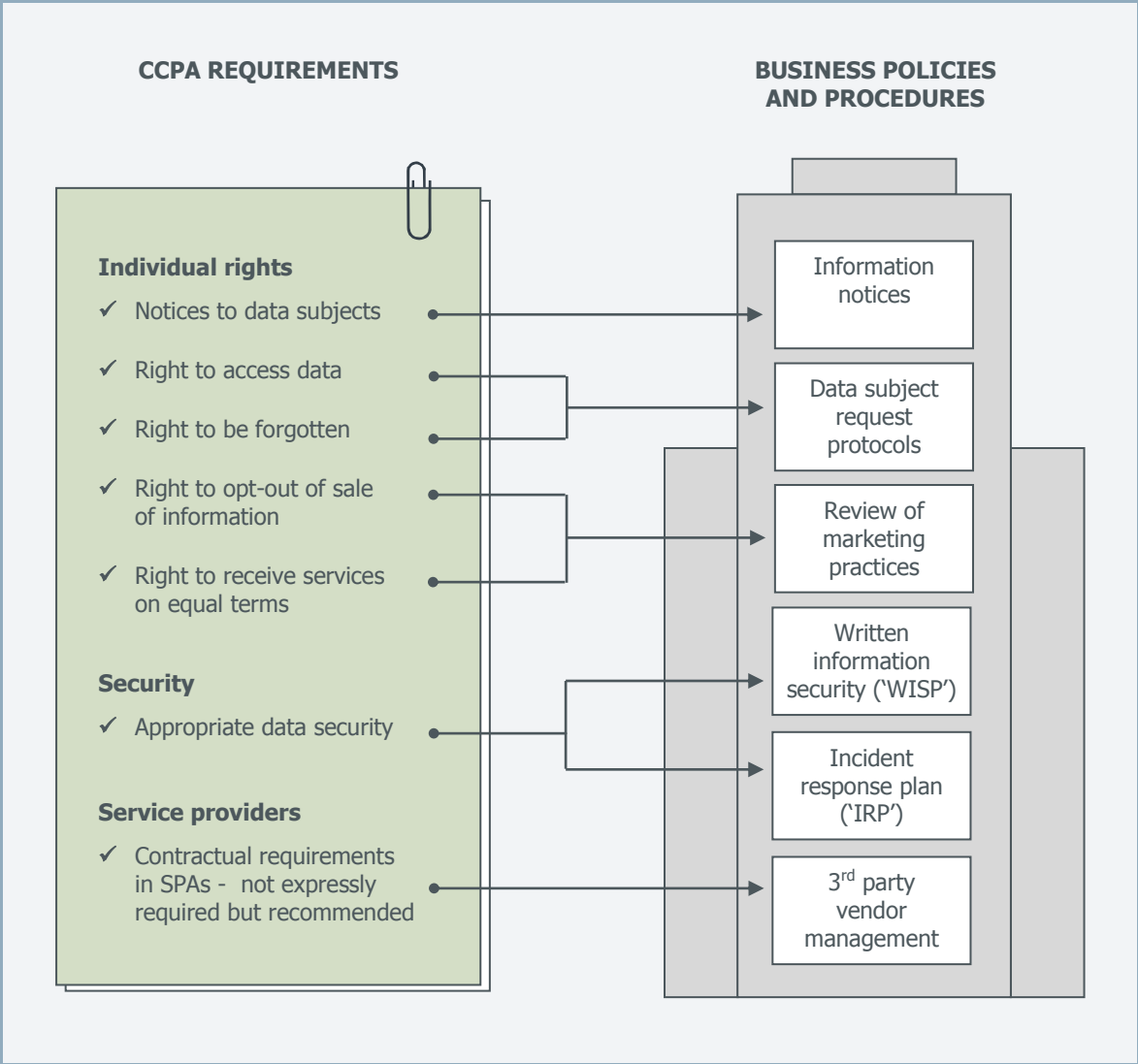


Unlike many other data privacy and security statutes, the CCPA also carves out from most of its provisions

- Non-profits that do not operate for “profit or financial benefit.”
- Financial institutions that are regulated under the Gramm-Leach-Bliley Act.
- Consumer reporting agencies that are regulated under the Fair Credit Reporting Act.
- Health care providers that are regulated by the Health Insurance Portability and Accountability Act.

SUMMARY OF COMPLIANCE REQUIREMENTS

The CCPA’s requirements can be grouped into three “buckets” –those that relate to individual rights, those that relate to data security, and those that relate to service providers. The following provides a cross reference between the core requirements of the CCPA and the functional policies and procedures that organizations should consider putting into place as part of their compliance strategy.



Cross References

CCPA Provisions
Cal. Civ. Code § 1798.100(b) Cal. Civ. Code § 1798.100(a) Cal. Civ. Code § 1798.105 Cal. Civ. Code §§ 1798.115(d), 1798.120 Cal. Civ. Code § 1798.125(a)(1) Cal. Civ. Code § 1798.150(a)(1)

PRIVACY NOTICES

A privacy notice (sometimes referred to as a privacy policy or an information notice) is a document provided by a company to data subjects that includes, among other things, a description of what types of personal data the company collects, how the company uses that data, with whom the company shares the data, and how the company protects the data.

The CCPA requires that a business provide those Californians about whom it has collected personal information, information about the organization’s privacy practices. The privacy notice should typically be given “at or before the point of collection” of the information.




Comparison to Other Privacy Laws

Prior to the enactment of the CCPA there were several laws within the United States and within other countries – most notably the European General Data Protection Regulation (“GDPR”) – that required companies to publish a privacy notice. The CCPA differs from those laws in the following respects:

BUSINESS REQUIREMENTS	US federal laws	Most US state laws	GDPR	CCPA
Applies to a broad range of companies and not limited to distinct industries e.g. finance	x	x	✓	✓
Applies to the collection of personal information online and offline	◇	x	✓	✓
Provide detailed information on how they use and process the personal information they collect	◇	x	✓	✓
Notify individuals about a right to access information they hold about them	◇	x	✓	✓
Notify individuals about a right to have their information deleted	◇	x	✓	✓
Include a ‘Do not sell my personal information’ link on websites and privacy notices	x	x	x	✓
Describe the information that they share with service providers	x	x	x	✓
Describe the types of entities to whom they sell information	x	x	✓	✓

◇ Requirement exists in some contexts, but not in others.

Compliance To Do List

	Review existing privacy notices and verify that they meet each of the new requirements of the CCPA.
	Identify instances in which you may be collecting information about Californians and do not currently have a privacy notice.
	In such situations, draft a privacy notice that conforms with both the CCPA and with other privacy laws that may apply (e.g., the GDPR).

How We Can Help

BCLP looks at privacy notices the same way regulators and class action attorneys do– with an eye toward spotting inconsistencies, errors, and facial violations of the law.

We also bring to bear a deep understanding of how other organizations have addressed the challenges of conveying complex privacy concepts in a simple outward facing document. We can validate that a privacy policy – whether it was originally drafted to comply with United States or European law – complies with all of the new requirements of the CCPA.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.100(b) (disclosure required at point of collection) Cal. Civ. Code § 1798.110(c) (contents of privacy notice)	Recital 58 (discussion of transparency principle) Recital 60 (discussion of contents of privacy notice) Recital 61 (discussion of timing of privacy notice) Recital 62 (discussion of redundancy of information) Article 12 (prohibition on charging for privacy information) Article 13 (privacy notice requirements for direct collection of personal data) Article 14 (privacy notice requirements for indirect collection of personal data)

RIGHT TO ACCESS DATA

The right to access data refers to the ability of a person to request that a business confirm whether it has personal information about him or her, the type of personal information that the business keeps about the individual, and/or a copy of the specific information that the business has on file. Access requests are sometimes referred to as Data Subject Access Requests, DSARs, or SARs.

Comparison to Other Privacy Laws

The right of access is not a new concept. For example, the European Union Charter of Fundamental Rights, which was adopted in 2000, states that “[e]veryone has the right of access to data which has been collected concerning him or her” That right was further codified in the European Privacy Directive of 1995 and, more recently, in the GDPR. The majority of data privacy laws in the United States do not include a right to access personal data, but there are some notable exceptions. For example, the Health Insurance Portability and Accountability Act (“HIPAA”) and the Family and Educational Rights and Privacy Act (“FERPA”) confer rights of access in the context of health related data and student records.

Compliance To Do List

	Review existing methods for submitting access requests to your organization to verify that they comply with the CCPA.
	Review existing policies or procedures for authenticating individuals that make access requests.
	If no authentication policy exists, draft an appropriate policy for authentication of individuals that make data subject requests.
	Draft a “play book” that provides standard communications that can be sent to individuals that make access requests, and standard formats for reporting personal information.
	Train employees on the handling of access requests.
	Verify that the policy in-place facilitates the fulfillment of access requests within the time period permitted by the statute.

How We Can Help

Companies across the globe have retained BCLP to draft their internal protocols for handling consumer access requests, or to review existing protocols to spot red flags that might be of concern to a court or a regulator.

Cross References



















CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.100(a) Cal. Civ. Code § 1798.110(a)(1)-(5), (b) Cal. Civ. Code § 1798.130(a)(1)-(7)	Recital 58 Recital 63 Recital 64 Recital 68 Article 15 Article 20

RIGHT TO BE FORGOTTEN

The right to be forgotten (sometimes called the right of erasure or the right to deletion) refers to the ability of a person to request that a business delete the personal information that it holds about them. The right to be forgotten is often misinterpreted as being an absolute right when, in reality, it only applies in a limited number of situations.

Comparison to other privacy laws

The right to be forgotten is not a new concept and has long been a cornerstone of European data privacy law. Indeed, the right was included within the Privacy Directive which was put into place in 1995 and was carried over into the current GDPR. Like the CCPA, the GDPR confers a limited right to be forgotten. The following compares the exceptions to the exercise of the right under both laws.

TYPES OF INFORMATION	GDPR	CCPA
Information is necessary to complete a transaction requested by the data subject or to perform a contract		
Information is necessary to detect security incidents		
Information is necessary to protect against deceptive, fraudulent or illegal activity		
Information is necessary to identify and repair errors		
Information is necessary to promote free speech		
Information is necessary for scientific, historical or statistical research in the public interest.		
Information is necessary for internal uses of a company, if those uses are reasonable expected by consumers		
Information is necessary to comply with a legal obligation.		
Information is used internally in a manner that is compatible with the context of the collection.		



Deletion is not required



Deletion may be required in some circumstances.

While the majority of United States data privacy laws do not include a right to be forgotten, the Children’s Online Privacy Protection Act (“COPPA”) has an analogous provision. COPPA regulates the online collection of information from children under the age of 13. Pursuant to the rules implementing COPPA, parents have a right to review “or have deleted the child’s personal information.” In addition to COPPA, California previously enacted what is often referred to as the “Eraser Button Law” that permits children under the age of 18 to delete or de-identify information that they posted online.

Compliance To Do List

<input checked="" type="checkbox"/>	Review existing methods for submitting deletion requests to your organization to verify that they comply with the CCPA.
<input checked="" type="checkbox"/>	Review existing policies or procedures for authenticating individuals that make deletion requests.
<input checked="" type="checkbox"/>	If no authentication policy exists, draft an appropriate policy for authentication of individuals that make data subject requests
<input checked="" type="checkbox"/>	Draft a "play book" that provides standard communications that can be sent to individuals that make deletion requests.
<input checked="" type="checkbox"/>	Train employees on the handling of deletion requests.
<input checked="" type="checkbox"/>	Verify that the policy in-place facilitates the fulfillment of deletion requests within the time period permitted by the statute.
<input checked="" type="checkbox"/>	Review protocols for deleting personal information.
<input checked="" type="checkbox"/>	Review technological capability for doing a "hard delete" (i.e., an irrevocable deletion) and a "selective deletion" (i.e., deleting one individual's information without corrupting a larger information system) from live systems.

How we can help

Companies across the globe have retained BCLP to draft their internal protocols for handling consumer requests for deletion, or to review existing protocols to spot any red flags that might be of concern to a court or a regulator.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.105(a), (d)(1)-(9)	Recital 65 Recital 66 Article 17

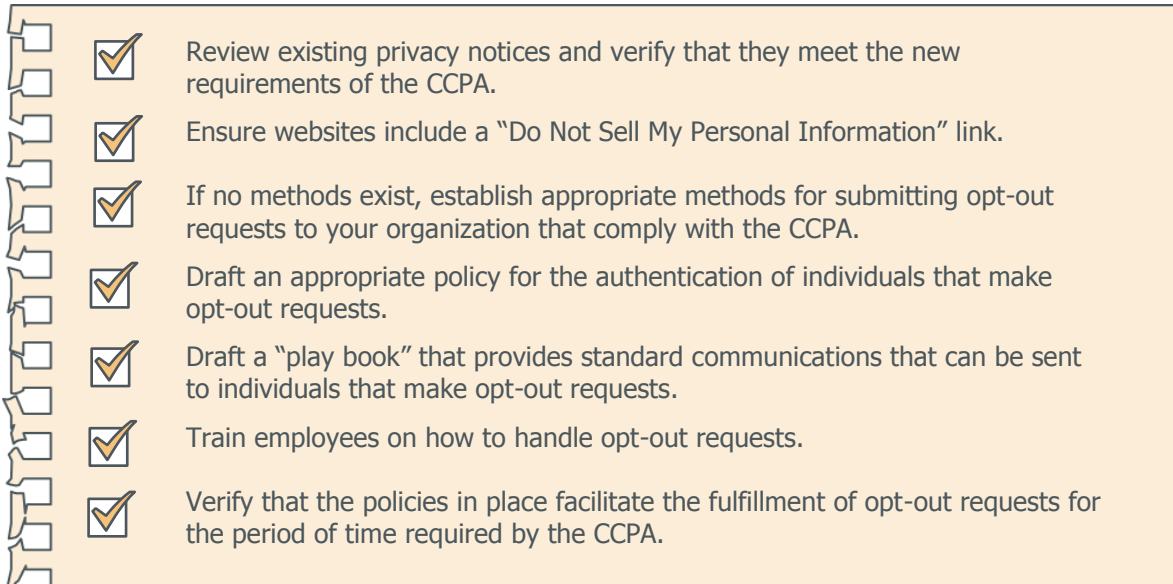
RIGHT TO OPT-OUT FROM HAVING INFORMATION SOLD

The right to opt-out refers to the ability of a person to direct that a business cannot sell the personal information that it holds about them.

Comparison to Other Privacy Laws

The CCPA is not the first law to confer upon individuals a right to opt-out from an organization’s use or disclosure of their information. Other federal laws, including the Gramm-Leach-Bliley Act (“GLBA”) and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (“CAN-SPAM Act”) contain certain opt-out requirements. Similarly, the GDPR confers a limited right to object to processing of personal data in certain circumstances, or to revoke consent. Notably, however, none of these privacy laws specifically address selling personal information.

Compliance To Do List



- Review existing privacy notices and verify that they meet the new requirements of the CCPA.
- Ensure websites include a “Do Not Sell My Personal Information” link.
- If no methods exist, establish appropriate methods for submitting opt-out requests to your organization that comply with the CCPA.
- Draft an appropriate policy for the authentication of individuals that make opt-out requests.
- Draft a “play book” that provides standard communications that can be sent to individuals that make opt-out requests.
- Train employees on how to handle opt-out requests.
- Verify that the policies in place facilitate the fulfillment of opt-out requests for the period of time required by the CCPA.

How We Can Help

Companies across the globe have retained BCLP to draft their internal protocols for handling consumer opt-out requests, or to review existing protocols to spot red flags that might be of concern to a court or a regulator.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.120	Recital 69 Recital 70 Article 7 Article 21

RIGHT TO OPT-IN TO HAVING INFORMATION SOLD (MINORS)

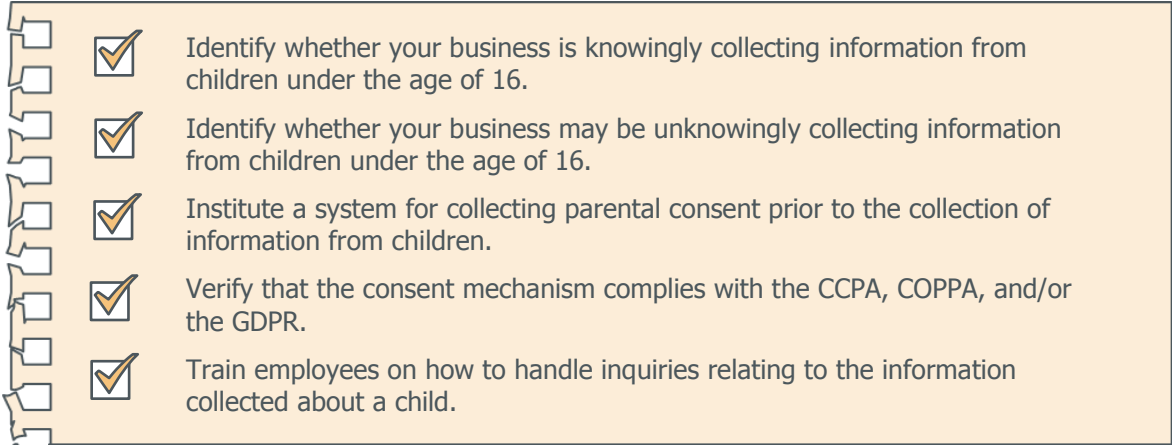
The right to opt-in refers to the requirement within the CCPA that a business cannot sell the personal information of a consumer that is less than 16 years old unless the business has received "opt-in" consent – i.e., affirmative authorization for the sale of the information. If a child is between the ages of 13 and 16 they can provide the necessary opt-in consent directly to the business. If a child is under the age of 13, a parent or guardian must provide the consent.

Comparison to Other Privacy Laws

The CCPA is not the first law to require that an organization obtain opt-in consent before taking certain actions with respect to information. In the United States the Children’s Online Privacy Protection Act ("COPPA") requires that companies inform parents about whether the company discloses a child’s information to third parties (e.g., whether they sell the information) and then obtain the opt-in consent of a parent or guardian. Unlike the CCPA, COPPA only applies to information collected from children who are under the age of 13.

In Europe, the GDPR requires that an "information society service" may not collect information from a child under the age of 16 unless it inform parents about whether the company discloses a child’s information to third parties and then obtains the opt-in consent of a parent or guardian. Member States are permitted to enact their own legislation that lowers the age requiring parental consent to 13 –functionally emulating the age requirement of COPPA.

Compliance To Do List



- Identify whether your business is knowingly collecting information from children under the age of 16.
- Identify whether your business may be unknowingly collecting information from children under the age of 16.
- Institute a system for collecting parental consent prior to the collection of information from children.
- Verify that the consent mechanism complies with the CCPA, COPPA, and/or the GDPR.
- Train employees on how to handle inquiries relating to the information collected about a child.

How We Can Help

Companies across the globe have retained BCLP to draft their internal protocols for handling consumer opt-in requests, or to review existing protocols to spot red flags that might be of concern to a court or a regulator.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.120(d)	Article 8

RIGHT TO RECEIVE SERVICES ON EQUAL TERMS

The “right to equal service and price” refers to the CCPA’s prohibition against discriminating against consumers who exercise their rights under the CCPA. Where a consumer exercises a right, a business is prohibited from denying goods or services, charging a different price, imposing penalties, providing a different level or quality of service, or suggesting the consumer will receive a different price or rate or different level or quality of goods or services.

Comparison to Other Privacy Laws

While the majority of data privacy laws in the United States do not include anti-discrimination provisions, the CCPA is not the first to broach the topic. For example, the Health Insurance Portability and Accountability Act (“HIPAA”) directly addresses the issue of genetic discrimination.

Compliance To Do List

- Review your business’s pricing policies and practices to verify that they do not price discriminate – intentionally or inadvertently – based upon whether a person opts-out of the sale of their information.
- Review existing privacy notices and verify that they meet the new requirements of the CCPA.
- Draft an appropriate policy for managing requests by consumers who exercise their rights under the CCPA.
- Train employees on how to handle and document requests by consumers who exercise their rights under the CCPA.
- Verify that policies in place facilitate compliance with the new requirements of the CCPA for consumers who exercise their rights.

How We Can Help

Companies across the globe have retained BCLP to draft internal protocols, or to review existing protocols to spot red flags that might be of concern to a court or a regulator.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.125(a)(1)	None





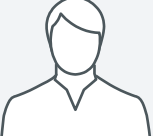


DATA SECURITY

The CCPA requires that organizations put into place “reasonable security procedures and practices” to help protect personal information from being breached. If information is breached and the breach happens “as a result of” an organization’s failure to implement reasonable security, the statute permits impacted individuals to bring suit to recover a statutory liquidated damage of between \$100 and \$750 per consumer per incident.







Comparison to Other Privacy Laws

There are over thirty statutes in the United States that require that companies take steps to protect personal information. Indeed, California Civil Code 1798.81.5 – which predated the CCPA by almost 15 years – contains a near identical standard to that used within the CCPA. The only significant change that the CCPA makes to the existing data security law within California is the prospect that a plaintiff may be able to recover statutory damages that exceed any real harm that he/she actually incurred.

From an international perspective, while California’s security standard is nearly equivalent to that used within the GDPR, it shows a clear preference for private class action enforcement whereas the GDPR incentivizes enforcement through supervisory authorities.

	GDPR	CCPA
 <p>STANDARD FOR PROTECTING DATA</p>	<p>“. . . the controller and the processor shall implement <i>appropriate technical and organizational measures to ensure a level of security appropriate to the risk . . .</i>”</p>	<p>“A business . . . shall implement and maintain <i>reasonable security procedures and practices appropriate to the nature of the information</i>, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”</p>
 <p>REGULATORY PENALTY</p>	 <p>Up to the greater of 2% of total worldwide annual turnover or €10million</p>	 <p>\$7,500 for each violation</p>
 <p>LIABILITY TO IMPACTED INDIVIDUAL</p>	 <p>Compensation for damages suffered</p>	 <p>Up to the greater of \$750 per consumer per incident or actual damages</p>

Compliance To Do List

-  Memorialize security policies and procedures in a written information security plan or "WISP."
-  Review whether your WISP conforms to a known industry standard or framework.
-  Consider whether there are any security policies or procedures that have not been drafted, but should be included within your WISP.
-  Review the substance of your WISP on an annual basis.
-  Conduct periodic risk assessments to identify the primary risks to information.
-  Train employees on your security policies and procedures.

How We Can Help

Companies across the globe have retained BCLP to review their WISP to spot anything that might be considered a red flag to a plaintiff’s attorney, a court, or a regulator.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.81.5(b) (pre-existing California security standard) Cal. Civ. Code § 1798.150(a)(1) Cal. Civ. Code § 1798.155(b)	Article 32(1) Article 83(4)(a) Article 82(1)


SERVICE PROVIDER AGREEMENTS

The CCPA allows businesses to share personal information with third parties or service providers for business purposes so long as there is a written contract that complies with the CCPA. Among other things, the CCPA prohibits any agreement or contract provision that seeks to waive or limit a consumer’s rights under the CCPA.

Comparison to Other Privacy Laws

Similar to the CCPA, the GDPR imposes certain requirements when a company uses a service provider. Both the CCPA and the GDPR require companies to contractually limit the service provider’s uses of personal information and to ensure the same restrictions that apply to the company will flow down to the service provider.

Compliance To Do List



- Review existing agreements with service providers to identify potential gaps.
- Identify instances in which you may be using a service provider that has access to information about Californians and with whom you do not currently have agreements in place.
- Update agreements with service providers to ensure that they meet the new requirements of the CCPA.

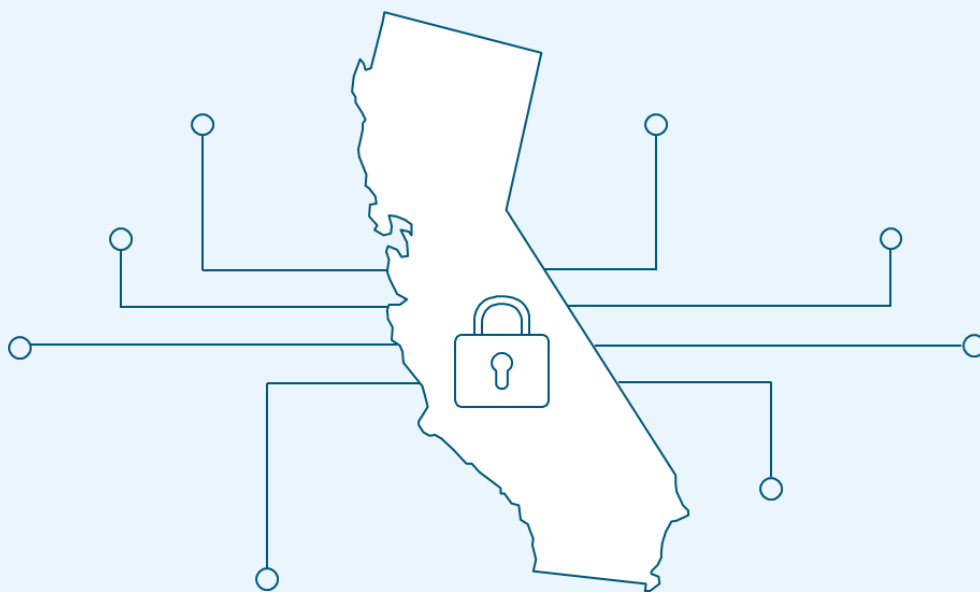
How We Can Help

Companies across the globe have retained BCLP to draft service provider agreements, or review their service provider agreements to spot anything that might be considered out of compliance with legal or regulatory requirements.

Cross References

CCPA Provisions	GDPR Provisions
Cal. Civ. Code § 1798.140(v), (w) Cal. Civ. Code § 1798.145(h)	Recital 81 Article 28

TEXT OF THE CCPA



Text of the California Consumer Privacy Act of 2018

(Last updated Sept. 23, 2018)

Table of Contents¹

1798.100 - Consumers right to receive information on privacy practices and access information
1798.105 - Consumers right to deletion
1798.110 – Information required to be provided as part of an access request
1798.115 – Consumers right to receive information about onward disclosures
1798.120 – Consumer right to prohibit the sale of their information
1798.125 – Price discrimination based upon the exercise of the opt-out right
1798.130 – Means for exercising consumer rights
1798.135 – Opt-out link
1798.140 – Definitions
1798.145 – Interaction with other statutes, rights, and obligations
1798.150 – Civil actions
1798.155 - Attorney General guidance and enforcement
1798.160 - Consumer privacy fund
1798.175 - Intent, scope, and construction of title
1798.180 - Pre-emption
1798.185 - Adoption of regulations
1798.190 - Intermediate steps or transactions to be disregarded
1798.192 - Void and unenforceable provisions of contract or agreement
1798.194 - Liberal construction of title
1798.196 - Construction with federal law and California constitution
1798.198 - Operative date

¹ Section headings do not appear in the official version of the statute and were added by BCLP for ease and clarity.

1798.100 - Consumers right to receive information on privacy practices and access information

- (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, in a 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 - Consumers right to deletion

- (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, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's 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 his or her 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 businesses' 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 - Information required to be provided as part of an access request

- (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 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 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 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 - Consumers right to receive information about onward disclosures

- (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 third party 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 - Consumer right to prohibit the sale of their information

- (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 between 13 and 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 - Price discrimination based upon the exercise of the opt-out right

(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 consumer 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 consumer by the consumer's data.
- (2) A business that offers any financial incentives pursuant to subdivision (a), shall notify consumers of the financial incentives pursuant to Section 1798.135.
- (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 1798.135 which 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 - Means for exercising consumer rights

- (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) 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, and if the business maintains an Internet Web site, a Web site address.
 - (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's 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's 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 shall not require the consumer to create an account with the business in order to make a verifiable consumer request.

- (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 Web site, and update that information at least once every 12 months:
 - (A) A description of a consumer's rights pursuant to Sections 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's privacy practices or the business's compliance with this title are informed of all requirements in Sections 1798.110, 1798.115, 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's 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 – Opt out link

- (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 - Definitions

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 such 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' 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' 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 the personal information that 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 Web site and any Internet Web page 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 1798.145, 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 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 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 Web site, 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. section 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 these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" 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 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 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.
 - (B) 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.

- (3) 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 1798.110 and 1798.115 if the business cannot verify, pursuant 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 - Interaction with other statutes, rights, and obligations

- (a) The obligations imposed on businesses by this title shall not restrict a business's 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) This title shall not apply to the sale of personal information to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined by subdivision (d) of Section 1681a of Title 15 of the United States Code, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).
- (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) Notwithstanding a business's 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.
- (h) 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.
- (i) This title shall not be construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.
- (j) 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.
- (k) 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.

1798.150- Civil actions

- (a)
- (1) Any consumer whose nonencrypted or 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 - Attorney General guidance and enforcement

- (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 - Consumer privacy fund

- (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 - Intent, scope, and construction of title

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 -Preemption

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 - Adoption of regulations

- (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 paragraph (1) of subdivision (a) of Section 1798.145.

- (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' determination that a request for information received by 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 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 - Intermediate steps or transactions to be disregarded

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 - Void and unenforceable provisions of contract or agreement

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' sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

1798.194 - Liberal construction of title

This title shall be liberally construed to effectuate its purposes.

1798.196 - Construction with federal law and California constitution

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 - Operative date

- (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 - Operative date

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

DATA PRIVACY AND SECURITY TEAM



David Zetoony
Partner / Chair Privacy Team
Corporate
T: +1 303 417 8530
david.zetoony@bcplaw.com



Kate Brimsted
Partner
Security, Corporate
T: +44 (0)20 3400 3207
kate.brimsted@bcplaw.com



Sarah Delon-Bouquet
Counsel
Litigation and Corporate Risk
T: +33 (0) 1 44 17 77 25
sarah.delonbouquet@bcplaw.com



Jena Valdetero
Partner
Litigation and Corporate Risk
T: +1 312 602 5056
jena.valdetero@bcplaw.com



Dominik Weiss
Counsel
Litigation and Corporate Risk
T: +49 (0) 40 30 33 16 148
dominik.weiss@bcplaw.com



Nicola Conway
Associate
Corporate
T: +44 (0) 20 3207 1312
nicola.conway@bcplaw.com



Tom Evans
Associate
Corporate
T: +44 (0)20 3400 2661
tom.evans@bcplaw.com



Jason Haismaier
Partner
Corporate
T: +1 303 417 8503
jason.haismaier@bcplaw.com



Josh James
Associate
Litigation and Corporate Risk
T: +1 202 508 6265
josh.james@bcplaw.com



Andrew Klungness
Partner
Corporate
T: +1 310 576 2176
andrew.k@bcplaw.com



Carolyn Krampitz
Associate
Corporate
T: +49 (0) 40 30 33 16 149
carolyn.krampitz@bcplaw.com



Emmanuelle Mercier
Associate
Litigation and Corporate Risk
T: +33 (0) 1 44 17 77 74
emmanuelle.mercier@bcplaw.com



François Alambret
 Counsel
 Litigation and Corporate Risk
 T: +33 (0) 1 44 17 77 48
francois.alambret@bcplaw.com



Jessica Pedersen
 Associate
 Litigation and Corporate Risk
 T: +1 312 602 5027
jessica.pedersen@bcplaw.com



Karin Ross
 Associate
 Corporate
 T: +1 303 417 8511
karin.ross@bcplaw.com



Tyler Thompson
 Associate
 Corporate
 T: +1 303 866 0231
tyler.thompson@bcplaw.com



Maria Vathis
 Of Counsel
 Litigation and Corporate Risk
 T: +1 312 602 5127
maria.vathis@bcplaw.com



Serena Yee
 Counsel
 Corporate
 T: +1 314 259 2372
sfyee@bcplaw.com

Getting in touch

When you need a practical legal solution for your next business opportunity or challenge, please get in touch.

David Zetoony

Tel: +1 303 417 8530

david.zetoony@bclplaw.com