CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

ANSWERS TO THE MOST FREQUENTLY ASKED QUESTIONS CONCERNING SERVICE PROVIDERS

April 2019

bclplaw.com

BRYAN CAVE LEIGHTON PAISNER BCLP

Content

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

INTRODUCTION

When the CCPA was enacted last year, BCLP published a Practical Guide to help companies reduce the requirements of the Act to practice. We followed the publication of the Guide with a series that addressed companies' most frequently asked questions concerning the CCPA. The series contributed to JD Supra naming BCLP as the 2019 "Top" law firm in the legal area of Data Collection & Data Use (i.e., data privacy).

One of the greatest areas of confusion caused by the CCPA is what impact the Act will have on service providers. In order to address that topic, we have collected our FAQs that specifically deal with the interaction between a business and its service providers and have republished them here in order to provide a "handbook" that companies can use when trying to understand how the CCPA impacts the relationships formed with service providers.

Sincerely,

David Zetoony

Bryan Cave Leighton Paisner

Chair Global Data Privacy and Security Practice

FAQ 1. ARE ALL VENDORS CONSIDERED "SERVICE PROVIDERS" UNDER THE CCPA?

No.

In order to be considered a "service provider" for the purposes of the CCPA, a legal entity must process personal information "on behalf of a business."[1] In addition, the vendor must be bound by a written contract that prohibits it from

1. retaining the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[2]
2. using the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[3] or
3. disclosing the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title."[4]

As a result there are a number of situations in which a business may use a vendor that does not qualify as a "service provider" under the CCPA. These include situations where:

- no written contract exists between a business and a vendor.
- a contract exists, but it allows the vendor to retain personal information beyond termination.
- a contract exists, but it allows the vendor to use personal information (in any form) for its own purpose.
- a contract exists, but it allows the vendor to make decisions about the disclosure of personal information.

In comparison, the European GDPR does not use the term "service provider" and, instead, refers to "processors." While processors within the GDPR are defined in a similar manner to "service providers" within the CCPA, the GDPR is far more proscriptive regarding the contractual terms that must be present in a processor agreement. Specifically, the GDPR requires that a controller and a processor clearly set forth the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data involved, the categories of

---

1 CCPA, Section 1798.140(v).
2 CCPA, Section 1798.140(v).
3 CCPA, Section 1798.140(v).
4 CCPA, Section 1798.140(v).

data subjects involved, the obligations and the rights of the controller, and the following substantive provisions:

1. Documented Instructions. The service provider will only process personal data consistent with the controllers documented instructions.[5]

2. Confidentiality. The service provider must ensure that persons authorized to process personal data have committed themselves to confidentiality.[6]

3. Processor Security. The service provider must implement appropriate technical and organizational measures to secure the personal data that it will be processing.[7]

4. Subcontracting authorization. The service provider must obtain written authorization before subcontracting, and must inform its client before it makes any changes to its subcontractors.[8]

5. Subcontracting flow down obligations. The service provider will flow down these obligations to any sub-processors.[9]

6. Subcontracting liability. The service provider must remain fully liable to the controller for the performance of a sub-processor's obligations.[10]

7. Responding to data subjects. The service provider will assist its client to respond to any requests by a data subject.[11]

8. Assisting Controller In Responding to Data Breach. The service provider will cooperate with its client in the event of a personal data breach. [12]

9. Assisting Controller In Creating DPIA. The service provider will cooperate with its client in the event the client initiates a data protection impact assessment.[13]

---

5 GDPR, Article 28(3)(a).
6 GDPR, Article 28(3)(b).
7 GDPR, Article 28(1), (3)(c); GDPR, Article 32(1).
8 GDPR, Article 28(2), 28(3)(d).
9 GDPR, Article 28(3)(d) Art. 28(4).
10 GDPR, Article 28(3)(d).
11 GDPR, Article 28(3)(e), GDPR, Article 12-23.
12 GDPR, Article 28(3)(f); GDPR, Article 33-34.
13 GDPR, Article 28(3)(f); GDPR, Article 35 – 36.

10. Delete or return data. The service provider will delete or return data at the end of the engagement.[14]

11. Audit Right. The service provider will allow its client to conduct audits or inspections for compliance with these obligations.[15]

12. Cross-border transfers. The service provider will not transfer data outside of the European Union without permission from its client.[16]

---

14 GDPR, Article 28(3)(g).

15 GDPR, Article 28(3)(h).

16 GDPR, Article 28(3)(a); GDPR, Article 46

FAQ 2. CAN AN INDEPENDENT CONTRACTOR BE CONSIDERED A "SERVICE PROVIDER" UNDER THE CCPA?

Yes.

The CCPA defines a "service provider" as being 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 . . . ."[17] Independent contractors are typically sole proprietors, although in some instances they may elect to create a limited liability company ("LLC") or an S-corporation in order to help protect their personal assets from liability. Regardless of the legal form that the independent contractor takes, they can technically be classified as a "service provider" if they meet the other restrictions imposed by the CCPA as discussed in FAQ 1.

---

[17] CCPA, Section 1798.140(v).

FAQ 3. IS A SERVICE PROVIDER PERMITTED TO DISCLOSE PERSONAL INFORMATION IF IT RECEIVES A CIVIL SUBPOENA, OR A DISCOVERY REQUEST?

The CCPA was put together quickly (in approximately one week) as a political compromise to address a proposed privacy ballot initiative that contained a number of problematic provisions. (For more on the history of the CCPA, you can find a timeline that illustrates its history and development on page two of BCLP's Practical Guide to the CCPA). Given its hasty drafting there are a number of areas in which the Act is at best ambiguous, and at worst leads to unintended results. The ability of a service provider to respond to a civil subpoena or to respond to a discovery request is one of those issues.

Section 1798.140(v) of the CCPA states that a service provider must be contractually prohibited from "disclosing the personal information [provided to it by a business] 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*. . . ."[18] Section 1798.145(a) of the CCPA contains six exceptions in which the disclosure prohibitions within the Act would not apply. While one of those exceptions involves compliance with "a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities," the exception applies only to a "business."[19] As the Act defines "businesses" and "service providers" separately (the former determines the "purposes and means of the processing of consumer personal information, the latter does not) it appears that, on its face, the CCPA does *not* excuse a service provider from complying with its contractual obligation to not disclose information in order comply with civil investigations, subpoenas, or summonses. This conclusion is bolstered by the fact that one of the other exceptions within Section 1798.145(a) (an exception that allows for disclosure when cooperating with law enforcement agencies) specifically references service providers.

While common sense suggests that a service provider should be able to comply with a lawfully issued subpoena or discovery request, given the text of the CCPA, judicial guidance will be needed to determine whether businesses can contractually permit their service providers to comply with civil discovery and, if they cannot, whether a service provider will be permitted to disclose information in response to validly issued discovery without being held in breach of contract.

---

18 CCPA, Section 1798.140(v).

19 CCPA, Section 1798.145(a)(3).

FAQ 4. CAN A SERVICE PROVIDER USE AND TRANSFER PERSONAL INFORMATION IF THEY ANONYMIZE OR AGGREGATE IT?

Yes.

Section 1798.140(v) of the CCPA states that a service provider must be contractually prohibited from "retaining, using, or disclosing the personal information [provided to it by a business] for any purpose other than for the specific purpose of performing the services specified in the contract for the business."[20] The CCPA also states, however, that nothing within it restricts the ability of a business to "collect, use, retain, sell, or disclose consumer information" that is "*deidentified* or in the *aggregate* consumer information."[21] The net result is that if a service provider has an interest in retaining, using, or disclosing the information that it receives from a client, the service provider can anonymize or aggregate the information in order to convert it from "personal information" (for which there are retention, use, and disclosure restrictions) to non-personal information (for which the CCPA imposes no such restrictions).

Anonymized data, sometimes referred to as "de-identified" data, refers to data that "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer."[22] While there are a number of strategies for converting a file that contains personal information into one that does not, the CCPA requires that a business that uses de-identified information take the following four steps to help ensure that the data will not be re-identified:[23]

1. Implement technical safeguards that prohibit reidentification. Technical safeguards may include the process, or techniques, by which data has been de-identified. For example, this might include some combination of hashing, salting, or tokenization.
2. Implement business processes that specifically prohibit reidentification. This might include an internal policy or procedure that prevents employees or vendors from attempting to reidentify data.
3. Implement business processes to prevent inadvertent release of deidentified information. Among other things, this might include safeguards to help prevent de-identified information from being accessed or acquired by unauthorized parties.

---

20 CCPA, Section 1798.140(v).

21 CCPA, Section 1798.145(a)(5) (emphasis added).

22 CCPA, Section 1798.140(h).

23 CCPA, Section 1798.140(v).

4. Make no attempt to reidentify the information. As a functional matter, this entails that a business follow the policies that it enacts that prohibit reidentification.

It should be noted that the standard for "anonymization" or "de-identification" under the CCPA arguably differ from the standard for anonymization under the European GDPR. While the CCPA considers information that cannot "reasonably" identify an individual as anonymous, the Article 29 Working Party interpreted European privacy laws as requiring that data has been "irreversibly prevent[ed]" from being used to identify an individual.[24]

Aggregation is defined within the CCPA as 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."[25] In common parlance, it refers to the situation where multiple consumer data points are combined so as to prevent the extrapolation of data as it relates to any particular consumer. For example, if Mary lives 5 miles from Company A, and Peter lives 10 miles from Company A, an aggregate value (e.g., consumers live, on average, 7.5 miles from Company A) cannot be used to extrapolate the distance of Mary or Peter from Company A.

From a practical standpoint, if a service provider intends to retain, use, or share anonymized or aggregated information, the parties should consider including within the service provider agreement a definition of "anonymization" and "aggregation" that matches the definitions of those terms used within the CCPA.

---

[24] Article 29 Working Party, WP 216: Opinion 05/2014 on Anonymisation Techniques at 7, 20 (adopted 10 April 2014).

[25] CCPA, Section 1798.140(a).

FAQ 5. WHEN WOULD A "SERVICE PROVIDER" BE CONSIDERED A "BUSINESS" FOR THE PURPOSES OF THE CCPA?

An entity is considered a "business" under the CCPA when it determines the "purposes and means" of the processing of personal information, and falls under one of the volume thresholds set out by the Act – i.e., it has annual gross revenue exceeding $25 million, transactions of personal information relating to 50,000 or more individuals, or it derives at least 50% of its revenue from the sale of personal information.[26] In contrast, a service provider processes personal information "on behalf of a business" and is bound by a written contract prohibiting it from

1. retaining personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[27]

2. using personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[28] or

3. disclosing personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title."[29]

While there is no judicial or regulatory interpretation within California as to when a company determines the "purposes and means" of processing, it is conceivable that a California court could interpret a service provider that breaches contractual prohibitions against retention, use, or disclosure as functionally determining the purpose and means of processing. Were that to occur, the service provider would not necessarily convert itself into a "business" for the purposes of the CCPA and thus be subject to the obligations imposed by the Act upon businesses. For example, if a service provider was found to determine the purpose and means of processing, but still fell below the volume thresholds, then it might fall outside both the definition of a "service provider," and the definition of a "business" under the Act.

---

26 CCPA, Section 1798.140(c)(1).

27 CCPA, Section 1798.140(v).

28 CCPA, Section 1798.140(v).

29 CCPA, Section 1798.140(v).

In comparison, under the European GDPR, the Article 29 Working Party provided significant guidance concerning when a vendor might move outside the definition of "processor" and become a "controller." This shift can occur when a vendor makes decisions about how and why data will be processed by it determining (jointly or independently with its client) the purpose and means of processing. While the analysis depends upon a variety of factors, if the service provider makes any of the following decisions there is a reasonable likelihood that a European supervisory authority would consider it to be a "controller:"

- What the data will be used for.
- What data elements will be processed.
- How long the data will be stored.
- Who is to have access to the data.

Unlike the CCPA, the GDPR does not impose any volume thresholds that must be met before an entity can be classified as a "controller."

FAQ 6. DOES A UNITED STATES SERVICE PROVIDER HAVE TO COMPLY WITH THE CCPA, EVEN IF ITS CLIENT IS NOT SUBJECT TO THE ACT?

No.

The CCPA imposes obligations only upon "businesses" and not upon "service providers." Indeed, the only impact that the CCPA has upon service providers is indirect insofar as the Act requires a business that falls under its jurisdiction to impose certain contractual provisions upon its service providers (e.g., prohibitions on the use, retention, or disclosure of personal data). If a business does not, itself, fall under the jurisdiction of the CCPA, then any data that it sends to a service provider within California should not be impacted by the Act. For example, if a French company sends data about French nationals to a service provider located in California, neither the French company, nor the California service provider, should be governed by the CCPA.

In comparison, the European GDPR applies to companies that process data "in the context of the activities of an establishment . . . in the Union."[30] Therefore, to the extent that a service provider processes data in the context of its establishment in the European Union it is subject to the GDPR regardless of whether its client (i.e., the data controller) is itself subject to the GDPR. So, for example, if an American company that is not subject to the GDPR transmits data to a service provider in Europe, the European service provider is independently "required to comply with the obligations imposed on processors by the GDPR."[31]

The net result is that data sent to a European processor by an American company that is not subject to the GDPR receives the GDPR's processor-imposed protections, but does not receive the GDPR's controller-imposed protections. From a functional standpoint this means that the European processor should:

- enter into a contract with its client that satisfies the requirements of Article 28 of the GDPR (except that the contract does not need to include provisions that are designed to help a controller satisfy controller-imposed obligations under the GDPR).
- not process data except on instructions from its client, unless required to do so by Union or Member State law.
- maintain a record of all categories of processing carried out on behalf of its client pursuant to Article 30(2) of the GDPR.

---

30 GDPR, Article 3(1) (emphasis added).

31 EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation (16 Nov. 2018) at 9.

- cooperate with European supervisory authorities upon request.
- implement technical and organizational measures to ensure an appropriate level of security.
- notify its client without undue delay after becoming aware of a personal data breach.
- designate a data protection officer (if needed).
- take steps to comply with restrictions on the cross-border transfer of information.[32]

[32] EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation (16 Nov. 2018) at 11.

FAQ 7. WHAT IS A "DATA PROCESSING ADDENDUM?"

"Data processing addendum" or "DPA" has become a term of art to refer to an amendment to a master services agreement that is designed to bring a service provider's contract into compliance with the service provider or processor requirements of the CCPA and/or the GDPR.

FAQ 8. IF A SERVICE PROVIDER HAS ALREADY AGREED TO A DATA PROCESSING ADDENDUM THAT COMPLIES WITH THE GDPR, IS A BUSINESS REQUIRED TO RENEGOTIATE THE CONTRACT AGAIN FOR THE CCPA?

No.

Article 28 of the GDPR requires that a controller "bind[]" every service provider to approximately thirteen substantive provisions; it also requires that contracts with service providers contain specific disclosures concerning the type of processing that will be covered by the agreement. In order to comply with this requirement many companies put in place data processing addendum or "DPA's" which were designed to amend master service agreements to conform to the GDPR.

As discussed in FAQ 1, the CCPA requires that a service provider agree to three substantive restrictions involving their retention, use, and disclosure of personal information. While the CCPA does not mandate that a business include any other provisions in an agreement with a service provider, in order for a business to comply with its own obligations under the CCPA it must "push down" certain obligations onto its service providers. For example, if a business is required to delete a consumer's personal information pursuant to a right to be forgotten request, the business will be unable to comply with that requirement if its service provider is unable to selectively and irrevocably delete data. The following chart compares the requirements that the GDPR imposes upon processors with those that a business should impose upon a service provider pursuant to the CCPA. As the chart indicates, a DPA that complies with all of the GDPR requirements will also satisfy each of the CCPA's requirements.

Requirement	GDPR	CCPA
Particulars :		
1. Subject Matter. Description of the subject matter of processing.	✓ Art. 23(3)	X
2. Duration. Description of the duration of processing.	✓ Art. 23(3)	X
3. Nature and Purpose. Description of the nature and purpose of processing.	✓ Art. 23(3)	X
4. Type of Data. Description of the type of personal data to be processed.	✓ Art. 23(3)	X
5. Categories of Data. Description of the categories of data subjects about which the data relates.	✓ Art. 23(3)	X

Requirement	GDPR	CCPA
Restrictions		
6. Use Restrictions. A service provider can only process personal data consistent with a controller's documented instructions.	✓ Art. 28(3)(a)	✓ § 1798.140(v)
7. Disclosure Restrictions. Confidentiality provision that ensures that persons authorized to process personal data have committed themselves to confidentiality.	✓ Art. 28(3)(b)	✓ § 1798.140(v)
8. Delete or return data. Service provider will delete or return data at the end of the engagement.	✓ Art. 28(3)(g)	✓ § 1798.140(v)
Security		
9. Security. Service provider will implement appropriate technical and organizational measures to secure information.	✓ Art. 28(1) Art. 28(3)(c) Art. 32(1)	X
10. Assisting Controller In Responding to Data Breach. Service provider will cooperate with controller in the event of a personal data breach.	✓ Art. 28(3)(f) Art. 33 – 34	X (although other California laws apply to data breach response)
Subprocessing		
11. Subcontractor selection. A service provider must obtain written authorization before subcontracting, and must inform the Company before it makes any changes to its subcontractors.	✓ Art. 28(2) Art. 28(3)(d)	X
12. Subcontracting flow down obligations. Service provider will flow down these obligations to any subprocessors.	✓ Art. 28(3)(d) Art. 28(4)	X
13. Subcontracting liability. A service provider must remain fully liable to the controller for the performance of a sub-processors obligations.	✓ Art. 28(3)(d)	X

Requirement	GDPR	CCPA
Data Subject / Consumer Requests		
14. Responding to data subjects. Service provider will assist the Company in responding to any requests by a data subject.	✓ Art. 28(3)(e) Art. 12 – 23	✓ § 1798.105(c) (relating to deletion)
Miscellaneous		
15. Assisting Controller In Creating DPIA. Service provider will cooperate with controller in the event the controller initiates a data protection impact assessment.	✓ Art. 28(3)(f) Art. 35 Art. 35-36	X
16. Audit Right. Service provider will allow Company to conduct audits or inspections for compliance to these obligations.	✓ Art. 28(3)(h).	X
17. Cross-border transfers. Service provider will not transfer data outside of the EEA without permission of Company.	✓ Art. 28(3)(a) Art. 46	X

FAQ. 9 WERE BUSINESSES REQUIRED TO PUT "DATA PROCESSING ADDENDUM" IN PLACE BY JANUARY 1, 2019?

No.

Some law firms reported that the CCPA required businesses to update their vendor agreements before 2019 (i.e., by December 31, 2018) in order to avoid having to characterize the transfer of personal information to vendors as "selling personal information" when the CCPA goes live on January 1, 2020. Their rationale was that Section 1798.130(a)(4)(B) of the CCPA requires that a company "[i]dentify by category . . . the personal information of the consumer that the business sold in the preceding 12 months" (i.e., going back to January 1, 2019) and that the CCPA's broad definition of the term "sell" might implicate many service providers.

While the CCPA broadly defines the term "sell" as including disclosures of personal information "for monetary or other valuable consideration," it is doubtful that the definition would extend to most vendors for four reasons.[33]

First, when a business discloses information to a service provider it typically does not do so to receive "monetary" consideration – to the contrary, in most situations the business must provide monetary consideration to a service provider, not the other way around. While one might argue that the business is receiving "other valuable consideration" (in the form of services), there is a strong argument that the business is not receiving the other valuable consideration in return for the personal information that it provides; rather the "other valuable consideration" is being provided in return for payment to the service provider.

Second, the CCPA states that a business that shares information with a service provider in order to have a business purpose performed is not "selling" the information if "the service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose."[34] Put differently, if a vendor is prohibited from using the personal information for its own purposes then the transmission is not considered a "sale." This dovetails with the CCPA's definition of "service provider" which, as is discussed in FAQ 1, requires that the vendor agree to three substantive restrictions involving the retention, use, and disclosure of personal information. As a practical matter the vast majority of vendor agreements already contain a restriction that personal information can only be used to provide a service to the client. As a result, for many (if not most) service provider agreements little change would be needed. Furthermore, for those areas in which a vendor may be using information for their own purposes (e.g., to improve a product or service generally) there is

---

33 CCPA, Section 1789.140(t)(1).

34 CCPA, Section 1798.140(t)(2)(C).

insufficient guidance concerning how the CCPA will be interpreted to know definitively whether such uses would cause the transfer of data to fall within the definition of a "sale."

Third, if the business has already negotiated a data processing addendum with the vendor for the purposes of the GDPR, that addendum should, as is discussed in FAQ 7, fulfill all of the requirements within the CCPA to classify the vendor as a "service provider:"

Requirement	GDPR	CCPA
Restrictions		
Use Restrictions. A service provider can only process personal data consistent with a controller's documented instructions.	✓ Art. 28(3)(a)	✓ § 1798.140(v)
Disclosure Restrictions. Confidentiality provision that ensures that persons authorized to process personal data have committed themselves to confidentiality.	✓ Art. 28(3)(b)	✓ § 1798.140(v)
Delete or return data. Service provider will delete or return data at the end of the engagement.	✓ Art. 28(3)(g)	✓ § 1798.140(v)

Fourth, assuming that a vendor could be characterized as providing valuable consideration to a business "for" the personal information that it receives (i.e., that it is being sold the personal information), and assuming that the vendor's contract does not, as of January 1, 2019, have a clear contractual use limitation, nothing within the CCPA prevents businesses and vendors from negotiating contractual addendum in 2020 with retroactive effect.

The net result is that a vendor agreement only had to be revised by December 31, 2018, if all of the following conditions were met: (1) the vendor paid its client for personal information (or provided some other valuable consideration in exchange for personal information), (2) the existing services agreement permitted the vendor to use the information for its own purposes, (3) the vendor did not enter into a data processing addendum that complies with Article 28 of the GDPR, and (4) there was a high likelihood that the vendor would refuse in 2019 to amend its service provider agreement to retroactively clarify use, disclosure, and retention restrictions.

FAQ 10. CAN A BUSINESS UNILATERALLY AMEND A SERVICE PROVIDER AGREEMENT TO INCORPORATE REQUIREMENTS UNDER THE CCPA?

Sometimes.

As discussed in FAQ 1, a business is required to impose restrictions on their service providers' ability to use, retain, and disclose consumer personal information. Whether a business can impose a unilateral amendment upon a service provider (*i.e.,* simply declare that the service provider must abide by each of restrictions mandated by the CCPA) largely depends upon the structure of the underlying agreement. Specifically, if the underlying agreement grants the business the right to impose unilateral changes, or the right to impose unilateral data security or privacy standards, the unilateral amendment would likely be effective. If, however, the underlying agreement requires that any amendment be done through a writing signed by both parties, the unilateral amendment would likely be ineffective.

Some businesses attempt to leverage generic "compliance with law" provisions found in master service agreements to impose unilateral changes by arguing that the unilateral changes are necessary in order for the service provider to comply with the CCPA. While courts have not evaluated whether that strategy would be effective, because the CCPA does not impose obligations upon service providers directly, and requires only that such obligations be imposed via contract, a court may find that a service provider would be in compliance with the "law" (i.e., statutes) that apply directly to the service provider even if the service provider did not agree to those provisions necessary for its client to comply with those aspects of the CCPA that apply directly to the client.

The ability to amend a service provider agreement unilaterally to incorporate data privacy protections may be somewhat different where the service provider (or the client) is subject to the GDPR. Unlike the CCPA, the GDPR imposes obligations directly upon processors that are subject to its jurisdiction. As a result, there is a reasonable argument that a processor that fails to incorporate restrictions into its contract is, itself, violating the GDPR. As a result, in the context of the GDPR, the effectiveness of a unilateral modification strategy depends upon the following factors:

- What law is selected within the underlying agreement? Whether a unilateral amendment can be incorporated through an existing compliance

with law provision depends, in part, on the principles of contract interpretation under the law selected to govern the underlying agreement.

- What forum is selected within the underlying agreement? Whether a unilateral amendment can be incorporated through an existing compliance with law provision depends, in part, upon the court or tribunal selected to interpret the underlying agreement if a dispute were to arise.

- Does the unilateral amendment exceed the scope of the GDPR? Attempts by a controller to go beyond the precise wording of the GDPR would likely be considered ineffective by most courts or tribunals. For example, while the GDPR requires that a processor make itself available for audits, a unilateral amendment that attempts to demarcate the boundary and scope of such audits (*e.g.*, who will pay for the audit, how often audits might occur, etc.) may be rejected by courts.

- Is the processor directly governed by the GDPR? If the processor is not established within the EU, it may argue that it is not directly governed by the GDPR and, therefore, a generic reference to its "compliance with law" should not be interpreted as including the GDPR.

- Does the controller have prior knowledge that the processing does not comply with the provisions of Article 28? To the extent that the controller has actual knowledge that certain aspects of the processing are not in compliance with Article 28 (*e.g.,* subcontracting is already occurring, disclosed security measures are arguably deficient, inadequate instructions were provided by the controller, or the controller has provided an inadequate (or non-existent) description of the processing), some jurisdictions may refuse to enforce a unilateral amendment based upon the equitable principles of laches and estoppel.

- Does the unilateral amendment attempt to restrict the jurisdictions in which the processor can transfer data? A unilateral amendment that restricts the ability of the processor to transfer (or receive) data outside of the EEA will likely be ineffective if the processor is physically based outside of the EEA, and/or if the controller had knowledge that the processing would occur outside of the EEA.

FAQ 11. IF A DATA SUBJECT SUBMITS AN ACCESS OR DELETION REQUEST DIRECTLY TO A SERVICE PROVIDER, IS THE SERVICE PROVIDER REQUIRED TO RESPOND TO THE DATA SUBJECT?

The CCPA was put together quickly (in approximately one week) as a political compromise to address a proposed privacy ballot initiative that contained a number of problematic provisions. (You can find a timeline that illustrates the CCPA's history and development on page 2 of BCLP's Practical Guide to the CCPA). Given its hasty drafting there are a number of areas in which the act intentionally, or unintentionally, is at best ambiguous, at worst leads to unintended results. One of those areas involves how a service provider should respond to a request by a consumer to access or delete their information.

The CCPA states that a consumer has the right to request that a "business that collects a consumer's personal information" disclose the "specific pieces of personal information . . . collected."[35] The term "business" is defined as any "legal entity" that is "operated for . . . profit" and 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 . . .

The most logical interpretation of the above definition is that the phrase "determines the purposes and means of the processing" applies both to (1) entities that collect personal information and (2) entities on behalf of which such information is collected. Under such an interpretation most service providers would not be considered a "business" to the extent that they do not determine the purpose and means of processing. That said, the definition of business appears to be missing a comma after the phrase "or on the behalf of which such information is collected." Absent the comma, it is unclear whether the clause "determines the purposes and means of the processing" applies *only* to entities "on the behalf of which such information is collected." If the purpose and means qualification only applies to entities on whose behalf information is collected, it might mean that service providers that directly collect consumer personal information fall under the definition of "business."[36]

---

35 CCPA, § 1798.100(a), 105(a).

36 A plaintiff's attorney might point to other references within the CCPA that appear to envision that service providers might receive, and have discretion when responding to, consumer requests. For example, the CCPA states that a "business *or a service provider* shall not be required to comply with a consumer's request to delete the consumer's personal information" in a number of enumerated circumstances. CCPA, § 1798.105(d). Of course the reference here to "service provider" could be referring to all service providers,

The CCPA also does not explain, or define, what it means to determine the "purpose and means of processing." While there is a great deal of interpretation of that phrase under European privacy law (which utilizes a similar phrase) it's unclear to what degree California courts will defer to European regulators when interpreting a California statute.

The net result is that while the best interpretation of the CCPA is one that holds that consumers have no right to request access or deletion of their personal information directly from service providers, the obtuse language of the CCPA leaves some uncertainty concerning whether California courts will adopt that interpretation.

Under the European GDPR, if a service provider is considered a "processor," as discussed in FAQ 1, the service provider is not required (or permitted) to substantively respond to a data subject's request to access, modify, or delete their personal data unless their client (the "controller") has specifically delegated the authority to act on their behalf in response to data subject requests. The service provider is required, however, to "assist[] the controller" when requested by the controller with the "controller's obligation to respond to requests" from the data subject.[37] As a practical matter, most European drafted data processing addendum require that a service provider forward a request that it receives from a data subject to the service provider's client for the client to determine how the request should be answered. If the client determines that the data subject is entitled to access their information, modify their information, or have their information deleted, the data processing addendum also typically requires the service provider to work with the client-controller to carry out that decision.

---

just those service providers that contribute to determining the purpose and means of processing, or service providers that receive an instruction from their client (as opposed to a request from a consumer) to provide or delete information.

[37] GDPR, Article 28(3)(e).

FAQ 12. ARE SERVICE PROVIDERS REQUIRED TO FULLY INDEMNIFY BUSINESSES FOR THEIR PROCESSING ACTIVITIES?

No. The CCPA does not mandate that a service provider indemnify a business (i.e., its client) for the service provider's activities in relation to the data. The CCPA allows a business and service provider to negotiate the degree to which one will (or will not) indemnify the other.

In contrast, the obligation of a service provider to indemnify its client is less clear under the European General Data Protection Regulation.

Processor liability is discussed within at least three sources of European data privacy law. First, Article 28(4) of the GDPR states that a service provider must "remain fully liable" to a controller for "the performance" of its *subprocessors'* "obligations."[38] It is important to note that this requirement of "full liability" for the performance of subprocessors may not need to be codified in the agreement between a controller and a processor. Specifically, Article 28 is structured such that the requirements of Article 28(3) must be included in the contract between the parties. Article 28(4), on the other hand, does not state that the controller-processor contract must include "full liability" language. The net result is that a processor must be liable for the performance of its subprocessors, but that liability does not need to be codified in the contractual relationship. It's also unclear whether supervisory authorities and courts will interpret liability for the "performance" of an obligation as indicating that the processor is liable for any damages caused by a subprocessors performance, or is simply liable for ensuring that the processing is performed by the subprocessor.

Second, a similar requirement concerning liability for the actions of subprocessors can be found within the Standard Contractual Clauses ("SCC"). The SCC for transfers from a controller to a processor are one of three mechanisms for transferring data from a controller in the European Economic Area to a processor that is neither located in the EEA, or in a country deemed to have laws that provide the same types of protections as the GDPR. Clause 11(1) of the controller-to-processor SCC provides that in the event the processor uses a subprocessor, and the subprocessor fails to fulfill its data protection obligations, the processor shall remain "fully liable" to the controller for the performance of the *subprocessor's* obligations. As with Article 28(4), Clause 11(1) of the SCC does *not* provide that processors must indemnify controllers for liability arising from their own actions, nor does it specify whether the liability referred to is for damages caused by the subprocessor or simply the performance of the agreed to processing activity.

---

[38] GDPR, Article 28(4).

Third, Article 82 of the GDPR states that "any person who has suffered material or non-material damage as a result of an infringement" by a processor of the regulation may receive compensation from that processor for the "damage suffered"[39] and that a "processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."[40] It is not clear whether the reference to a "person" in this section of the GDPR is intended to encompass natural persons (*i.e.*, data subjects) or natural persons and legal entities (*i.e.*, data subjects, and controllers). As a result, Article 82 may not require that a processor be "fully liable" for direct damages suffered by a controller as a result of its processing. If a data subject successfully obtains damages against a controller for the unlawful processing of a processor, the controller is permitted to "claim back from the . . . processors involved in the same processing that part of the compensation corresponding to [the processor's] part of responsibility for the damage . . . ."[41] The GDPR is silent as to whether the ability of a controller to claim contribution for third party damages can be waived, capped, or limited by contract.

The net result is that while the GDPR does not require that a processor *contractually* assume any liability, processors that enter into the SCCs must, at a minimum, assume liability for the "performance" of processing assigned to subprocessors. It remains to be seen whether the GDPR permits a controller to seek damages for any first party harm it incurs as a result of a processor's violation of the regulation, or prevents the parties from limiting the ability of the controller to seek indemnification for first party damages, or third party liabilities.

[39] GDPR, Article 82(1).
[40] GDPR, Article 82(2).
[41] GDPR, Article 82(5).

FAQ 13. ARE SERVICE PROVIDERS REQUIRED TO FULLY INDEMNIFY BUSINESSES FOR THE ACTIONS OF THEIR SUBCONTRACTORS?

No. The CCPA does not mandate that a service provider indemnify a business (i.e., its client) for the actions of the service provider's subcontractors. The CCPA allows a business and service provider to negotiate the degree to which one will (or will not) indemnify the other.

In contrast, the European General Data Protection Regulation does require that a service provider (i.e., a processor) indemnify its client (i.e., a controller) for some of the actions of its subcontractors.

The GDPR imposes two requirements when a company uses a service provider.

The first requirement is controllers must "bind[]" every service provider to, at a minimum, the thirteen substantive requirements found in Article 28 concerning the data that will be processed on behalf of a controller. Of those requirements only one addresses liability. Article 28(4) provides that a service provider must remain fully liable to the controller for the performance of a subprocessors' obligations.[42] It is important to note that this requirement of "full liability" for the performance of subprocessors may not need to be codified in the agreement between a controller and a processor. Specifically, Article 28 is structured such that the requirements of Article 28(3) must be included in the contract between the parties. Article 28(4), on the other hand, does not state that the controller-processor contract must include "full liability" language. The net result is that a processor must be liable for the performance of its subprocessors, but that liability does not need to be codified in the contractual relationship. If you are a controller, however, you will want to require that the data processing agreement expressly state that the processors will remain "fully liable" for each subprocessor's failure to fulfill its obligations thereunder in relation to the processing of any personal data.

The second requirement is that if a controller is based in the European Union and is transferring personal data to a processor that is based outside of the European Union, the parties must take steps to ensure that the jurisdiction to which the data is going affords the data "an adequate level of protection."[43] The United States, for example, is not considered to be a country that affords an adequate level of protection. Most companies satisfy this requirement by adopting contract provisions that have been pre-approved by the European Commission as guaranteeing an "adequate level of protective," *i.e.*, the Standard Contractual Clauses ("SCC"). Clause 11(1) of the controller-to-processor SCC provides that in

---

[42] GDPR, Article 28(4).
[43] GDPR, Article 45(1).

the event the subprocessor fails to fulfill its data protection the processor shall remain "fully liable" to the controller for the performance of the sub-processor's obligations. The SCC provide that the parties shall not vary or modify the clauses. Accordingly, companies utilizing the SCC are required to include this language holding processors liable for the performance of their subprocessors.

FAQ 14. IS A BUSINESS RESPONSIBLE IF ITS SERVICE PROVIDER MISUSES (OR MISAPPROPRIATES) PERSONAL INFORMATION?

No. As discussed above, in order to be considered a "service provider" for the purposes of the CCPA, a vendor must be bound by a written contract that prohibits it from

1. retaining the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[44]
2. using the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[45] or
3. disclosing the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title."[46]

If a business negotiates an agreement with a service provider that contains the three provisions above, but the service provider breaches the agreement by retaining, using, or disclosing the information for a purpose other than providing services to its client, the CCPA makes clear that the business "shall not be liable" so long "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."[47]

---

44 CCPA, Section 1798.140(v).

45 CCPA, Section 1798.140(v).

46 CCPA, Section 1798.140(v).

47 CCPA, Section 1798.145(h).

FAQ 15. IS A SERVICE PROVIDER RESPONSIBLE IF ITS CLIENT VIOLATES THE CCPA?

No. As discussed above, in order to be considered a "service provider" for the purposes of the CCPA, a vendor must be bound by a written contract that prohibits it from

1. retaining the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[48]
2. using the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title,"[49] or
3. disclosing the personal information "for any purpose other than for the specific purpose of performing the services specified in the contract . . . or as otherwise permitted by this title."[50]

If a service provider negotiates an agreement with a client that contains the three provisions above, the CCPA states that the service provider will "not be liable" in the event that its client fails to fulfill the client's obligations as a "business" under the Act.[51] So, for example, a service provider should not be liable if its client fails to post a privacy notice, inaccurately describes its sharing practices, or fails to disclose that it has transferred personal information to the service provider.

---

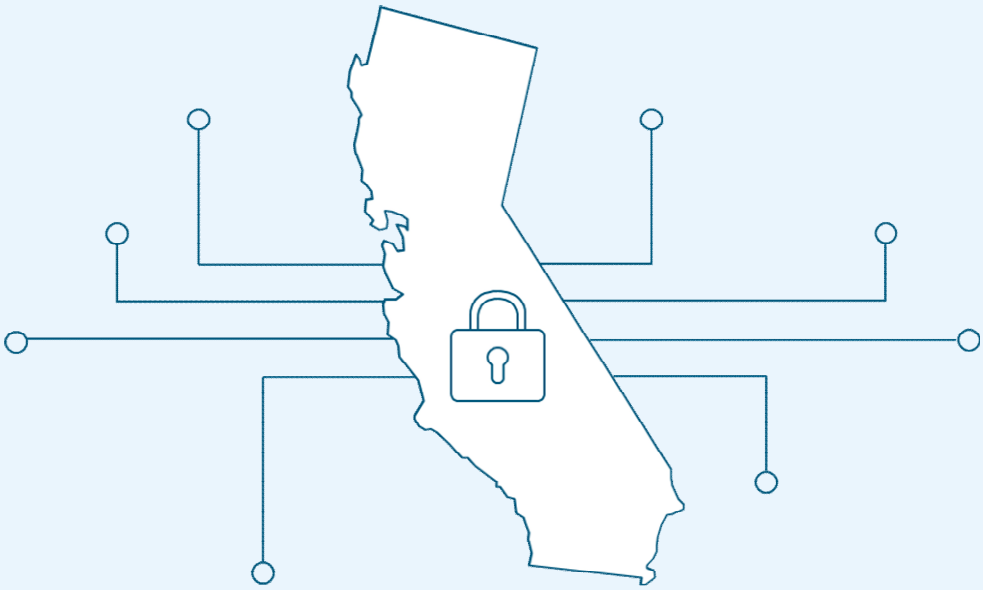
48 CCPA, Section 1798.140(v).

49 CCPA, Section 1798.140(v).

50 CCPA, Section 1798.140(v).

51 CCPA, Section 1798.145(h)

TEXT OF THE CCPA



Text of the California Consumer Privacy Act of 2018

(Last updated Sept. 23, 2018)

Table of Contents[52]

---

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

1798.100 – 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 - 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 – Substance of required disclosures

(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 - Right to receive access to information and 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 - 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 rights

(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, and additional disclosure requirements

(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
Boulder, Colorado
T: +1 303 417 8530
david.zetoony@bclplaw.com

Kate Brimsted
Partner
London, England
T: +44 (0)20 3400 3207
kate.brimsted@bclplaw.com

Sarah Delon-Bouquet
Counsel
Paris, France
T: +33 (0) 1 44 17 77 25
sarah.delonbouquet@bclplaw.com

Jena Valdetero
Partner
Chicago, Illinois
T: +1 312 602 5056
jena.valdetero@bclplaw.com

Dominik Weiss
Counsel
Hamburg, Germany
T: +49 (0) 40 30 33 16 148
dominik.weiss@bclplaw.com

Nicola Conway
Associate
London, England
T: +44 (0) 20 3207 1312
nicola.conway@bclplaw.com

Tom Evans
Associate
London England
T: +44 (0)20 3400 2661
tom.evans@bclplaw.com

Jason Haislmaier
Partner
Boulder, Colorado
T: +1 303 417 8503
jason.haislmaier@bclplaw.com

Josh James
Associate
Washington D.C.
T: +1 202 508 6265
josh.james@bclplaw.com

Andrew Klungness
Partner
Santa Monica, California
T: +1 310 576 2176
andrew.k@bclplaw.com

Carolyn Krampitz
Associate
Hamburg, Germany
T: +49 (0) 40 30 33 16 149
carolyn.krampitz@bclplaw.com

Emmanuelle Mercier
Associate
Paris France
T: +33 (0) 1 44 17 77 74
emmanuelle.mercier@bclplaw.com

François Alambret
Counsel
Paris, France
T: +33 (0) 1 44 17 77 48
francois.alambret@bclplaw.com

Jessica Pedersen
Associate
Chicago, Illinois
T: +1 312 602 5027
jessica.pedersen@bclplaw.com

Karin Ross
Associate
Boulder, Colorado
T: +1 303 417 8511
karin.ross@bclplaw.com

Tyler Thompson
Associate
Boulder Colorado
T: +1 303 866 0231
tyler.thompson@bclplaw.com

Maria Vathis
Of Counsel
Chicago, Illinois
T: +1 312 602 5127
maria.vathis@bclplaw.com

Serena Yee
Counsel
St. Louis, Missouri
T: +1 314 259 2372
sfyee@bclplaw.com

Kevin Scott
Counsel
Chicago, Illinois
T: +1 312 602 5074
kevin.scott@bclplaw.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