California Consumer Privacy Act ("CCPA") White Paper

October 1, 2018

DOMINIQUE SHELTON LEIPZIG | PARTNER
+1.310.788.3327
DSheltonLeipzig@perkinscoie.com

SARI RATICAN | SENIOR COUNSEL
+1.310.788.3287
SRatican@perkinscoie.com

LAURA MUJENDA | ASSOCIATE
+1.310.788.3309
LMujenda@perkinscoie.com

Table of Contents

Page

I. OPENING

Does your company process personal information of California residents (e.g., by using analytics on your website)? If so, it is imperative that you pay close attention to the California Consumer Privacy Act ("CCPA"), which goes into effect on January 1, 2020. The CCPA goes well beyond the European Union's General Data Protection Regulation ("GDPR"); however, if you have achieved compliance with the GDPR, you may be able to leverage your GDPR program to achieve CCPA compliance.

Once in effect, the CCPA will require businesses processing the personal information ("PI") of California consumers (defined as California residents) to comply with new regulations governing the processing of their PI. Businesses, that meet the statutory definition, will have to respond to eight specific consumer rights, observe restrictions on data monetization business models, and update their privacy notices to provide detailed disclosures about their data handling practices concerning California residents' PI.

II. BACKGROUND

The impetus for the CCPA was a growing concern regarding the volume of data collected about California consumers. In June 2018, a privacy initiative qualified for the ballot with 629,000 signatures, nearly twice the signatures required. To facilitate amendments and respond to heavy criticism regarding workability, the ballot initiative was withdrawn from the November 2018 ballot in exchange for California Assembly Bill ("AB") 375—the first iteration of the CCPA. On June 28, 2018, California Governor Brown signed AB 375 into law.

Shortly thereafter, California Senate Bill ("SB") 1121 was introduced to amend the CCPA in five ways: (1) eliminating the requirement that a consumer bringing a private right of action first notify the Attorney General; (2) including a carveout for providers of health care governed by the California Confidentiality of Medical Information Act; (3) including an exemption for business associates under the Health Insurance Portability and Accountability Act of 1996;[1] (4) carving out any conflicts with the California Financial Information Privacy Act;[2] and (5) limiting civil penalties assessed in an Attorney General action to not more than $2,500 per violation or $7,500 per intentional violation. On September 23, 2018, Governor Brown signed SB 1121 into law. Nevertheless, further amendments are likely forthcoming given that the current amendments do not address all the concerns raised by industry and consumer groups, as well as the California Attorney General, Xavier Becerra.

III. CCPA BASICS

The CCPA gives California consumers/residents[3] eight new privacy rights and imposes eight corresponding as well as three independent obligations on businesses processing California consumers' PI. Among other rights, it gives California consumers the right to request that a business provide the requesting consumer the categories and specific pieces of PI it collects about them, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which

[1]Cal. Civ. Code Section 1798.145(c)(1)(A)-(B).
[2]Cal. Civ. Code Section 1798.145(e).
[3]Cal. Civ. Code Section 1798.140(g) (defining "consumer" as a natural person who is a California resident); Cal. Code Regs. Tit. 18, Section 17014.

the information is shared. Further, consumers have a right to request a business that sells or discloses their PI for a business purpose to disclose the identity of third parties to which the information was sold or disclosed.

Under the CCPA, businesses must verify the requesting consumer's identity, promptly act on the consumer's request, and update their general privacy policy to include (among other items) a description of California consumers' rights, the purpose(s) of PI collection, and the categories of PI sold, collected or disclosed for a business purpose in the past 12 months. Businesses also have an obligation to provide the requested PI in a readily useable and portable format and respect consumers' choice to opt out of the sale of their PI. The CCPA prohibits businesses from discriminating against consumers who exercise their rights under the CCPA. Finally, the CCPA compels businesses to train employees, to create designated methods for consumers to assert their rights under the CCPA, and to execute written agreements with third-party data processors to prohibit selling, retaining, using, or disclosing the PI subject to the agreement.

The CCPA expands the definition of PI beyond the GDPR and well beyond current U.S. privacy law. It defines PI as "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*"[4] (emphasis added). The definition also includes personal identifiers; IP addresses; commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies; Internet or other electronic network activity information; professional or employment-related information; or any consumer profile.

In addition to the business obligations under the CCPA, businesses are provided with several general defenses and applicable specific exemptions to consumer requests and enforcement actions.

A. Eight Consumer Rights

The CCPA provides consumers with eight exercisable rights regarding their PI being held by a business as follows:

1. *Abbreviated Disclosure Right Applicable to Businesses that Collect PI* provides a consumer the right to request that a business disclose the categories and specific pieces of PI collected about them.[5]

2. *Expanded Disclosure Right Applicable to Businesses that Collect PI* provides a consumer the right to request that a business disclose the categories and specific pieces of PI collected, the sources from which the PI is collected, the business or commercial purpose (similar to legitimate interests under the GDPR) of collection, and with whom the collected PI is shared (i.e., third-party sharing).[6] Consumers have the right to receive a specific notice of

[4]Cal. Civ. Code Section 1798.140(o).
[5]Cal. Civ. Code Section 1798.100(a).
[6]Cal. Civ. Code Section 1798.110(a).

the business's PI collection practices[7] as well as notice of these rights within the business's general privacy policy.

3. *Right to Request Information from Businesses that Sell or Disclose PI for a Business Purpose* provides consumers the right to request that a business disclose the following for the previous 12 months: the categories of PI collected and sold, the categories of third parties to whom data is sold, and the categories of PI disclosed about the consumer for a business purpose.[8] Consumers have the right to receive specific notice of the business's PI collection practices as well as notice of these rights within the business's general privacy policy.[9]

4. *Right to Opt Out of the Sale of Data* gives consumers or their authorized agent the ability to direct businesses to stop selling their PI to third parties.[10] Consumers have the right to receive notice of these rights within the business's general privacy policy, as well as a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," leading to an internet web page that enables a consumer to opt-out of the sale of the consumer's PI.[11]

5. *Right to Opt In for Children: Business Obligation Not to Sell Children's PI Without Affirmative Authorization* provides that a business must obtain the opt-in consent from a child (between ages 13-16) or the child's parent or guardian (if the child is under the age of 13) before selling the child's PI.[12]

6. *Deletion Right* gives consumers the right to request that a business delete their PI after receipt of a verifiable request.[13] In support of this right, consumers have the right to receive notice of their right to deletion within the business's general privacy policy.[14]

7. *Right to Access and Portability* provides consumers the right to access their PI after submitting a verifiable access request.[15]

8. *Right Not to be Discriminated Against for Exercising Any of the Consumer's Rights Under the Title* gives consumers the right to not be discriminated against for exercising their rights under the CCPA. Examples of discrimination include denying goods or services to the consumer,[16] charging different prices or rates for goods or services,[17] providing a different

---

[7] *Id.*; Cal. Civ. Code Section 1798.110(c); Legislative Digest at p. 91; Cal. Civ. Code Section 1798.130(a)(5)(B).
[8] Cal. Civ. Code Section 1798.115(a).
[9] Cal. Civ. Code Section 1798.115(c); Cal. Civ. Code Section 1798.130(a)(5)(C).
[10] Cal. Civ. Code Section 1798.120(a).
[11] Cal. Civ. Code Section 1798.135(a)(1)-(a)(2).
[12] Cal. Civ. Code Section 1798.120(c)-(d).
[13] Cal. Civ. Code Section 1798.105(a).
[14] Cal. Civ. Code Section 1798.105(b); Cal. Civ. Code Section 1798.130(a)(5)(A).
[15] Cal. Civ. Code Section 1798.100(d); Legislative Digest Section 2(i)(4).
[16] Cal. Civ. Code Section 1798.125(a)(1)(A).
[17] Cal. Civ. Code Section 1798.125(a)(1)(B).

level or quality of goods or services to the consumer,[18] or 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.[19]

B. Eight Corresponding Business Obligations

To support California consumers' new rights, the CCPA has imposed eight corresponding business obligations. In order to appropriately respond to each request, businesses should first verify the requesting consumer's identity and the validity of the request. Only upon successful verification, and satisfaction that applicable defenses do not apply, should businesses act upon the request-specific obligation(s).

1. *Obligation to Respond to Abbreviated Disclosure Request:* Once the requesting consumer's identity has been verified, and assuming no defenses apply, the business must disclose and deliver the categories and specific pieces of the consumer's PI collected in the 12 months preceding the request free of charge within 45 days of receiving the verifiable request (unless an extension of an additional 45 days is necessary and the consumer is given notice of the extension).[20] A business has the obligation to provide the categories of PI collected in a general notice to consumers within its stated privacy policy.[21] In addition to responding to the requested disclosure, a business must implement two or more designated methods for consumers to submit requests for information, including, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address.[22]

   Here, the CCPA goes beyond GDPR Article 13 by requiring identification of specific pieces of information about the consumer and requiring special notice to individual consumers outside of a privacy policy. And unlike GDPR Article 20, which entitles the data subject to "receive" the data, the CCPA's *Abbreviated Disclosure Right* only calls for the company to "disclose and deliver the required information."

2. *Obligation to Respond to Expanded Disclosure Request:* Once the requesting consumer's identity has been verified,[23] if defenses do not apply, the business must disclose and deliver the following information covering the 12 months preceding the request: the categories of PI collected,[24] the categories of sources from which PI is collected,[25] the business or commercial purpose for collecting or selling the PI[26] (similar to legitimate interests under the

[18]Cal. Civ. Code Section 1798.125(a)(1)(C).
[19]Cal. Civ. Code Section 1798.125(a)(1)(D).
[20]Cal. Civ. Code Section 1798.110(b); Cal. Civ. Code Section 1798.130(a)(2).
[21]Cal. Civ. Code Section 1798.100(b).
[22]Cal. Civ. Code Section 1798.130(a)(1); Cal. Civ. Code Section 1798.140(i).
[23]Cal. Civ. Code Section 1798.110(b); Cal. Civ. Code Section 1798.130(a)(3)(A).
[24]Cal. Civ. Code Section 1798.110(c)(1).
[25]Cal. Civ. Code Section 1798.110(c)(2).
[26]Cal. Civ. Code Section 1798.110(c)(3).

GDPR), the categories of third parties with whom the business shares PI,[27] and the specific pieces of PI the business collected about consumer.[28]

The information must be provided free of charge within 45 days of receiving the verifiable request (unless an extension of an additional 45 days is necessary and the consumer is given notice of the extension).[29] Disclosure must be made in writing and delivered[30] through the consumer's account with the business if the consumer maintains such an account, or via postal mail or electronically at the consumer's option, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.[31] A business must not require the consumer to create an account with the business to make a verifiable request.[32] A business also has the obligation to provide the categories of PI collected in a general notice to consumers within its stated privacy policy.[33] Lastly, a business must implement two or more designated methods for consumers to submit requests for information, including, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address.[34]

The notice of business purpose under the CCPA is similar to the GDPR's notice of legitimate interest. The CCPA requirement to disclose "the business or commercial purposes for collecting or selling PI" is similar to the GDPR requirement to disclose/notify data subject(s) if relying on legitimate interest to process PI.[35] The CCPA requirement to provide specific pieces of consumer PI collected "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance"[36] is similar to the GDPR Portability Right in Article 20. However, the GDPR is more restrictive: portability requests may be made only if the business's lawful basis for processing the PI is the data subject's consent[37] or contractual necessity.

3. *Obligation to Respond to Request for Information from Businesses that Sell or Disclose PI for a Business Purpose:* Once the requesting consumer's identity has been verified, subject to appropriate defenses, the business must create two separate lists covering the preceding 12 months: (1) PI sold; and (2) PI disclosed for a business purpose.[38] The information must be provided free of charge within 45 days of receiving the verifiable request (unless an extension of an additional 45 days is necessary and the consumer is given notice of the extension).[39] In addition to responding to the requested disclosure, a business must

---

[27]Cal. Civ. Code Section 1798.110(c)(4).
[28]Cal. Civ. Code Section 1798.110(a)(5).
[29]Cal. Civ. Code Section 1798.130(a)(2).
[30]*Id.*
[31]*Id.*
[32]*Id.*
[33]Cal. Civ. Code Section 1798.130(a)(2).
[34]Cal. Civ. Code Section 1798.130(a)(1); Cal. Civ. Code Section 1798.140(i).
[35]GDPR Art. 13(1)(d).
[36]Cal. Civ. Code Section 1798.130(a)(2).
[37]*Id.*; GDPR Art. 20(1)(a).
[38]Cal. Civ. Code Section 1798.130(a)(4)(B).
[39]Cal. Civ. Code Section 1798.130(a)(2).

implement two or more designated methods for consumers to submit requests for information, including, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address.[40] Lastly, a business that sells consumer PI or discloses it for a business purpose must disclose such within its online privacy policy.[41]

This right goes beyond GDPR Article 13 and requires notice of specific categories of data sold or disclosed that are relatable to specific consumers.[42]

4. *Obligation to Respond to Request to Opt Out of the Sale of Data:* Once the requesting consumer's (or consumer's authorized representative's[43]) identity has been verified, and assuming no general or specific defenses apply, the business must stop selling the consumer's data unless the consumer subsequently provides express authorization for the sale of the consumer's PI.[44] A business must 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 PI again.[45] An exception does exist for PI collected in connection with a consumer's exercise of an opt-out request if the PI is solely used for complying with the opt-out request.[46]

   This consumer right goes beyond GDPR Article 18, which is limited to the four circumstances where a user is contesting accuracy, lawfulness, use beyond a legal claim, or the legitimate interest reasoning.[47] Further, a business must provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," leading 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.[48] Under the definition of "home page," a business may include this notice either on its main home page or a separate home page dedicated to California consumers that discloses the California-specific description of their privacy rights.[49]

5. *Obligation to Respond to Obtain Opt-In Consent for Children:* Businesses are obligated to obtain opt-in consent before selling the PI of a child.[50] A business may obtain opt-in consent from a child, if the child is between the ages of 13 and 16.[51] A business must obtain opt-in consent from a child's parent or guardian for children under the age of 13.[52]

---

[40]Cal. Civ. Code Section 1798.130(a)(1); Cal. Civ. Code Section 1798.140(i).
[41]Cal. Civ. Code Section 1798.115(c); Cal. Civ. Code Section 1798.130(a)(5)(C).
[42]*Id.*; GDPR Art. 13.
[43]Cal. Civ. Code Section 1798.120.
[44]Cal. Civ. Code Section 1798.120(c).
[45]Cal. Civ. Code Section 1798.135(a)(5).
[46]Cal. Civ. Code Section 1798.135(a)(6).
[47]GDPR Art. 18.
[48]Cal. Civ. Code Section 1798.135(a)(1).
[49]Cal. Civ. Code Section 1798.135(b).
[50]Cal. Civ. Code Section 1798.120(c)-(d).
[51]*Id.*
[52]*Id.*

The requirement is similar to the GDPR. However, under the GDPR Article 8, parental (or guardian) opt-in consent is required for children under 16 years of age.[53]

6. *Obligation to Respond to Deletion Requests:* Once the consumer's deletion request has been verified, and assuming no defenses apply, the business must delete the consumer's PI. [54] The CCPA recommends that such deletion requests be fulfilled within 45 days.[55] Businesses also have an obligation to notify consumers of their deletion rights in a form that is reasonably accessible to consumers[56] via a general privacy notice or in a section specific to California privacy rights.[57] Additionally, businesses must implement two or more designated methods for consumers to submit requests for information, including, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address.[58] A business is not required to comply with a consumer's deletion request if the PI is necessary for specific enumerated reasons, including to complete a contractual transaction or provide a good or service requested by the consumer.[59]

   The CCPA's deletion right is broader than GDPR Article 17's provisions because the CCPA allows deletion requests to be made for any reason, whereas GDPR Article 17 allows erasure requests only in specific circumstances.[60] However, the deletion right under the CCPA is subject to more defenses for business. For example a company may defend against a deletion request if the data is needed to investigate a security incident, debug software, or it if needed for internal uses. [61]

7. *Obligations to Respond to Requests for Access and Portability:* Once the consumer's request has been verified, if no other defenses apply, the business must disclose and deliver free of charge the required information via post or electronically in a portable format within 45 days of receiving the verifiable request.[62] If PI is delivered electronically, it should be delivered in a readily useable format to the extent feasible so that the consumer may transfer his or her PI to another business without hindrance. A business is not required to provide PI to a consumer more than twice in a 12-month period.[63]

   This CCPA right is broader than the data portability right under GDPR Article 20 because data portability requests under the GDPR are limited to those in which the business's lawful basis for processing the PI is the data subject's consent or contractual necessity.[64]

---

[53]GDPR Art. 8.
[54]Cal. Civ. Code Section 1798.105.
[55]Cal. Civ. Code Section 1798.130(a)(2).
[56]Cal. Civ. Code Section 1798.135(a).
[57]Cal. Civ. Code Section 1798.105(b); Cal. Civ. Code Section 1798.130(a)(5)(A).
[58]Cal. Civ. Code Section 1798.130(a)(1).
[59]Cal. Civ. Code Section 1798.105(b).
[60]GDPR Art. 17.
[61]Cal. Civ. Code Section 1798.105(d).
[62]Cal. Civ. Code Section 1798.130(a)(2).
[63]Cal. Civ. Code Section 1798.100(d).
[64]GDPR Art. 20.

8. *Obligation Not to Discriminate Against Consumers Exercising Their CCPA Rights:* Businesses are prohibited from discriminating against consumers exercising their CCPA rights in the following ways: denying goods or services to such consumers;[65] charging different prices or rates for goods or services, including through the use of discounts or other benefits or by imposing penalties;[66] and providing a different level or quality of goods or services to consumers if they exercise their rights under the CCPA.[67] A business is allowed to charge a higher price/rate or provide a different level/quality[68] if the higher price/rate or different level/quality is reasonably or directly related to the value provided to consumers for their PI.[69] The CCPA also allows a business to offer financial incentives, including payments to consumers as compensation for the collection, sale or deletion of PI, so long as the business notifies consumers of the financial incentives, clearly describes the material terms of the financial incentive program,[70] and obtains their opt-in consent.[71] It is a best practice to place notice of financial incentives in a general privacy policy notice. However, a business may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious,[72] and consumers can revoke their consent at any time.[73] As a compliance best practice, if a business intends to offer financial incentives tied to the exchange of PI, it will be advisable to consider the value of the data associated with the promotion.

C. Independent Business Obligations

Under the CCPA, businesses also have the following independent obligations, not tied to a specific consumer right:[74]

1. *Train Employees*: The CCPA requires businesses to train employees handling consumer inquiries on the requirements related to CCPA-provided consumer rights and business obligations.[75] Businesses are also obligated to ensure that employees know how to direct consumers to exercise their rights under the law.[76]

2. *Create Designated Methods for Consumers to Assert Their Rights*: Businesses must create two or more designated methods for consumers to submit requests for information, including a toll-free telephone number and a website address if the business maintains a website.[77] "Designated methods for submitting requests" include a postal mailing address, email

[65]Cal. Civ. Code Section 1798.125 (a)(1)(A).
[66]Cal. Civ. Code Section 1798.125 (a)(1)(B).
[67]Cal. Civ. Code Section 1798.125 (a)(1)(C).
[68]Cal. Civ. Code Section 1798.125 (a)(2).
[69]Cal. Civ. Code Section 1798.125 (b)(1).
[70]Cal. Civ. Code Section 1798.125 (b)(3).
[71]*Id*.
[72]Cal. Civ. Code Section 1798.125 (b)(4).
[73]Cal. Civ. Code Section 1798.125 (b)(3).
[74]Cal. Civ. Code Section 1798.130(a); Cal. Civ. Code Sections 1798.140(i), (w)(2)(A).
[75]*Id.*
[76]*Id.*
[77]Cal. Civ. Code Section 1798.130(a).

address, Internet webpage or portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under the CCPA.[78]

3. *Execute Vendor Contracts Containing Specific Criteria*: Businesses that engage vendors to handle PI must execute written contracts with specific criteria with those vendors if they want to shift liability to the vendor for any violations of the CCPA caused by the vendor.[79] If the vendor is defined as a "service provider" under the CCPA, it must have a written contract that limits processing to the business purpose of the contract.[80] If the vendor is defined as a "person" under the statute, among other requirements, the contract should prohibit vendors from selling, retaining, using or disclosing the PI outside of the direct business relationship with the business.[81] The contract must also include a certification from the vendor that he/she understands the restrictions and will comply with them.[82]

   GDPR Article 28's vendor obligations are more expansive than those required by the CCPA. Specifically, GDPR Article 28 requires businesses and vendors to enter into data processing agreements whereby vendors attest that they will (i) only process personal data on the business's documented instructions; (ii) ensure that persons authorized to process data are subject to confidentiality obligations; (iii) take certain security measures; (iv) obtain consent for sub-vendors; (v) help respond to consumer-verified requests; (vi) help with data breach responses; (vii) return or destroy all data at the end of services; and (viii) provide information to demonstrate the business's compliance with the GDPR, including by allowing and contributing to audits. Businesses should review their vendor contracts to ascertain if they have the requisite language already to shift liability to their vendors or if amendments are necessary.

D. General Business Defenses

The CCPA provides businesses with seven general defenses to the required obligations. Specifically, a business may assert that (1) it is not a covered business under the CCPA; (2) it is not processing PI as defined under the CCPA; (3) it falls under one of the CCPA's applicable exemptions; (4) the consumer request is not verifiable; (5) the data was collected for a single, one-time transaction and was not sold or retained; (6) the request would require the business to re-identify or otherwise link information that is not maintained in a manner that would be considered PI; and (7) the action is by the vendor and the proper contractual language is contained in the vendor agreement.

E. Applicable Exemptions

In addition to the general defenses, the CCPA provides seven applicable exemptions for businesses, including, but not limited to (1) data processed pursuant to the federal Gramm-

[78] Cal. Civ. Code Section 1798.140(i).
[79] Cal. Civ. Code Section 1798.140(v); Cal. Civ. Code Section 1798.140(w)(2)(A).
[80] Cal. Civ. Code Section 1798.140(v).
[81] Cal. Civ. Code Section 1798.140(w)(2)(A).
[82] *Id*.

Leach-Bliley Act, [83] and (2) the exemption applicable to protected medical or health information that is governed by the California Confidentiality of Medical Information Act,[84] the Health Insurance Portability and Accountability Act [85] and the Health Information Technology for Economic and Clinical Health Act,[86] as well as information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects.[87]

IV. PENALTIES

The CCPA provides a private right of action for any consumer whose nonencrypted PI is subject to an unauthorized access, exfiltration, theft or disclosure as a result of the business's failure to implement and maintain reasonable security procedures and practices.[88] Consumers may (1) recover damages not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater; (2) seek injunctive or declaratory relief; and/or (3) seek any other relief the court deems proper.[89]

Prior to initiating any action, a consumer must give the business 30 days' written notice identifying the specific CCPA provisions that have been or are being violated.[90] No action may be initiated if the business cures the noticed violations within 30 days of receiving notice and gives the consumer an express written statement confirming that the violations have been cured and that no further violations will occur.[91] However, if the business violates the CCPA in breach of this express written statement, the consumer may initiate an action to enforce the statement and pursue statutory damages for each breach of the statement, as well as any other violation of the title that postdates the statement.[92] This statement seems to contradict other sections of the CCPA, which limit a consumer's private right of action to violations related to security breaches caused by a lack of reasonable security.[93] Hopefully, further amendments to the bill may provide more clarity on this issue.

V. AREAS OF INFLUENCE

The Attorney General ("AG") cannot bring an enforcement action until six months after the publication of the final regulations or until July 1, 2020, whichever is sooner.[94]

---

[83] Cal. Civ. Code Section 1798.145(e).
[84] Cal. Civ. Code Section 1798.145(c)(1)(A)-(B).
[85] *Id.*
[86] *Id.*
[87] Cal. Civ. Code Section 1798.145(c)(1)(C).
[88] Cal. Civ. Code Section 1798.150(a)(1).
[89] *Id.*
[90] Cal. Civ. Code Section 1798.150(b).
[91] *Id.*
[92] *Id.*
[93] Cal. Civ. Code Section 1798.150(c).
[94] Cal. Civ. Code Section 1798.185(a)(7)(c).

The CCPA calls for the AG to promulgate rules to effectuate the new law. [95] The rule-making process will afford many avenues for companies to have their voices heard. Watch our video to learn more about this process

Video Spotlight:
Let Your Voice Be Heard: Start With the New California Privacy Law

You may also submit comments regarding the rulemaking process on the Perkins Coie CCPA Business Comments Submission Portal. Please understand that submitting a comment to this portal cannot and does not create any attorney-client relationship between you or your company and Perkins Coie LLP. Perkins Coie is collecting these comments solely as an administrative convenience so that many comments can be gathered and sent to the California Attorney General's office in a collective fashion. Perkins Coie will not review, analyze for proper form, make any changes to, or otherwise edit any comments submitted and is solely acting as a conduit, not as an advocate or attorney relating to any of these comments. Since there is no attorney-client relationship with Perkins Coie, please do not submit any information to us which you or your company considers confidential.

If you would like to discuss engaging Perkins Coie as counsel for your company, please contact Dominique Shelton Leipzig, but any such engagement will be conditioned on our mutual agreement, checking and clearing conflicts and execution of an engagement letter. Thank you for your attention.

On the legislative front, businesses may want to get involved with the California Chamber of Commerce's lobbying efforts to influence legislative efforts.

VI. CONCLUSION

Before the CCPA goes into effect on January 1, 2020, businesses should prepare data inventories of all PI pertaining to California residents (including employees), households, and devices, as well as information sources, storage locations, usage, and recipients. Absent that discipline, CCPA compliance will not be possible. Further, more detailed requirements will be

[95] Cal. Civ. Code Section 1798.185.

enacted during 2019 as additional revisions are debated and the AG begins rulemaking drafting and implementation.

Dominique Shelton Leipzig | Partner

www.perkinscoie.com/DShelton/

Privacy and cybersecurity attorney Dominique Shelton Leipzig co-chairs the firm's Ad Tech Privacy & Data Management group. She provides strategic privacy and cyber-preparedness compliance counseling, and she defends, counsels and represents companies on privacy, global data security compliance, data breaches and investigations with an eye towards helping clients avoid litigation. Dominique frequently conducts training sessions for senior leadership, corporate boards and audit committees regarding risk identification and mitigation in the areas of privacy and cybersecurity.

She leads companies in legal assessments of data security, cyber preparedness and compliance with such regulations as the California Confidentiality of Medical Information Act (CMIA), the Health Insurance Portability and Accountability Act (HIPAA), the Video Privacy Protection Act (VPPA), the Children's Online Privacy Protection Act (COPPA) and the NIST Cybersecurity Framework.

Dominique has significant experience leading investigations related to data and forensic breaches. She has steered investigations for a range of companies, including national retailers, financial institutions, health and wellness enterprises, media companies and others.

Dominique also advises companies on global privacy and data security, particularly on the EU General Data Protection Regulation (GDPR). Her background includes advising on European, Asian and South American privacy and security compliance projects for U.S.-based and overseas companies. In addition, she counsels on strategies for related legal compliance and vendor management in cross-border transfers.

Sari Ratican | Senior Counsel

Sari Ratican's global privacy and data protection practice focuses on providing practical advice tailored to each client's unique needs. Her advice reflects her extensive in-house experience as the first Chief Privacy Officer for Amgen, Inc., the world's largest biotechnology company, where she built and implemented the company's global privacy program across more than 75 countries.

Sari is a Certified Information Privacy Professional (EU and US) and has been actively involved in several global privacy and data protection organizations, including the International Association of Privacy Professionals, the International Pharmaceutical Privacy Consortium and the International Pharmaceutical & Medical Device Privacy Consortium.

In addition to global privacy and data protection matters, Sari has extensive experience in disciplines including healthcare fraud and abuse, compliance and ethics. Prior to specializing in global privacy and data protection, Sari was in private practice as a corporate healthcare lawyer and was also Legislative Counsel for the American Medical Association's Government Relations Department, where she worked with national and state professional medical associations on various legislative matters at both the state and federal levels.

Laura Mujenda | Associate

Laura Mujenda maintains a broad-based commercial litigation practice that includes business, privacy, data security, investigations and soft IP matters. As part of her growing privacy practice, Laura counsels clients on GDPR compliance, including preparing Article 30 reports and conducting gap analysis. Laura is also engaged in policy framework as related to the California Consumer Privacy Act (CCPA).

In her litigation practice, Laura has experience bringing and defending claims for fraud, misrepresentation, breach of contract, tortious interference with a contract, and trademark, trade dress and copyright infringement. She has handled various aspects of civil litigation, including dispositive motion practice, pleadings, discovery, depositions, dispute resolution and trial preparation. She also been involved in investigations related to retaliation, sexual harassment, gender or pregnancy-based discrimination and enforcement actions.

Laura's pro bono practice focuses on representing immigrants in removal proceedings who seek lawful admission into the U.S. In that regard, Laura recently secured release on bond and a grant of Deferral of Removal under the Convention Against Torture for a native and citizen of Guatemala.