

**ORIGINAL**

1 NIELSEN MERKSAMER  
2 PARRINELLO GROSS & LEONI LLP  
3 Sean P. Welch, Esq. (S.B. No. 227101)  
4 David J. Lazarus, Esq. (S.B. No. 304352)  
5 2350 Kerner Boulevard, Suite 250  
6 San Rafael, California 94901  
7 Telephone: (415) 389-6800  
8 Facsimile: (415) 388-6874  
9 E-mail: swelch@nmgovlaw.com  
10 E-mail: dlazarus@nmgovlaw.com

**FILED/ENDORSED**  
MAR 30 2023  
By: A. Turner  
Deputy Clerk

8 NIELSEN MERKSAMER  
9 PARRINELLO GROSS & LEONI LLP  
10 Kurt R. Oneto, Esq. (S.B. No. 248301)  
11 1415 L Street, Suite 1200  
12 Sacramento, California 95814  
13 Telephone: (916) 446-6752  
14 Facsimile: (916) 446-6106  
15 E-mail: koneto@nmgovlaw.com

13 *Attorneys for Petitioner*  
14 California Chamber of Commerce

15 IN THE SUPERIOR COURT OF THE STATE OF CALIFORNIA  
16 IN AND FOR THE COUNTY OF SACRAMENTO

17 CALIFORNIA CHAMBER OF COMMERCE,

Case No. <sup>3</sup>4 - 2023 - 80004106

18 Petitioner,

Action Filed:

19 vs.

VERIFIED PETITION FOR WRIT  
OF MANDATE [C.C.P. § 1085]  
AND COMPLAINT FOR  
DECLARATORY AND  
INJUNCTIVE RELIEF [C.C.P. §§  
1060 & 526a]

21 CALIFORNIA PRIVACY PROTECTION  
22 AGENCY; JENNIFER M. URBAN,  
23 ALASTAIR MACTAGGART, LYDIA DE LA  
24 TORRE, and VINHCENT LE, in their official  
25 capacities as board members of the California  
26 Privacy Protection Agency; ROB BONTA, in  
27 his official capacity as Attorney General of the  
28 State of California; and DOES 1-100,

Respondents.

## INTRODUCTION

1  
2       1.     Proposition 24, the “California Privacy Rights Act of 2020,” adopted  
3 by California voters in November 2020, established sweeping new requirements  
4 regarding businesses’ collection, retention, and use of consumer data and created  
5 an entirely new state agency called the California Privacy Protection Agency  
6 (“CPPA” or the “AGENCY”). It also expressly required the AGENCY to adopt a  
7 mandatory set of final regulations on or before July 1, 2022, and provided a  
8 period thereafter of at least one year for California businesses to prepare for the  
9 new law, in reliance on those final regulations, before enforcement could begin  
10 on July 1, 2023:

11             [T]he timeline for adopting final regulations required by the  
12 act adding this subdivision shall be July 1, 2022. ...  
13 Notwithstanding any other law, civil and administrative  
14 enforcement of the provisions of law added or amended by this  
15 Act shall not commence until July 1, 2023, and shall only apply  
16 to violations occurring on or after that date. (Civ. Code §  
17 1798.185(d) [attached in full as Petition Exhibit (“Pet. Ex.”) 1].)

18       2.     The law required the AGENCY to adopt a complete set of final  
19 regulations in 15 new substantive areas by July 1, 2022, providing businesses  
20 with a one-year grace period prior to enforcement of those new rules. But, to  
21 date, the AGENCY still has not published a *single* final regulation, nearly *nine*  
22 *months* past the mandated deadline. The AGENCY has not sought a legislative  
23 extension, judicial relief from the deadline, or emergency rulemaking—all of  
24 which were available options. Instead, the AGENCY ignored the deadline. Yet,  
25 the AGENCY is preparing to begin enforcement on July 1, 2023, leaving  
26 businesses scrambling to manage complex new requirements across their  
27 systems and products for rules that are not yet finalized. In fact, the AGENCY  
28 has not even previewed in draft form many of the required regulations,  
seemingly taking the position that it can issue those rules whenever it wants

1 and leave businesses with little or no time to implement those regulations before  
2 they are enforceable. The AGENCY's piecemeal approach and disregard of  
3 statutory deadlines is regulation by fiat that effectively and improperly rewrites  
4 Proposition 24 and severely prejudices California businesses by depriving them  
5 of the one-year compliance grace period established in the plain language of  
6 Proposition 24.

7       3. While the AGENCY has not published a single final regulation to  
8 date, it has previewed expansive new obligations in a partial set of draft  
9 regulations, filed with the Office of Administrative Law. The draft  
10 regulations contain detailed, complex requirements totaling 66 pages that all  
11 businesses subject to the law must follow. Yet, because the AGENCY delayed  
12 adopting final regulations well past the deadline, and has continually altered  
13 its draft regulations throughout the rulemaking process, businesses have  
14 been unable to act with certainty as they take steps towards compliance.  
15 Instead, businesses have been stuck in limbo during this ongoing rulemaking  
16 process, raising thousands of pages of comments and questions with the draft  
17 regulations and waiting to see if and how the AGENCY addresses those  
18 comments. Given the AGENCY's decision to commence enforcement of  
19 Proposition 24 on July 1, 2023, notwithstanding its failure to publish  
20 final regulations by the statutory deadline and the one-year compliance period  
21 in Proposition 24, businesses are now facing, at most, a period of only three  
22 months to comply with an expansive set of new regulations.

23       4. Making matters worse, the draft regulations submitted to the Office  
24 of Administrative Law are themselves incomplete. Despite a clear statutory  
25 mandate, the AGENCY has not even issued proposed regulations regarding  
26 some of the most complicated new requirements of Proposition 24. These include  
27 cybersecurity audits, "risk assessments," and automated decision-making  
28 technology. These are completely novel legal requirements with potentially large

1 operational business impacts, yet businesses have not even had a sneak peek of  
2 what the rules will be. If and when those regulations are drafted, businesses will  
3 (it seems) be expected to comply on severely shortened notice, in direct  
4 contravention of Proposition 24. These brand new rules can reasonably be  
5 expected to require significant operational work (as they are new requirements),  
6 which Proposition 24 accounted for by giving businesses a year to prepare. But  
7 the AGENCY's failure to timely promulgate regulations in these critical areas  
8 means that businesses may have no grace period whatsoever.

9       5. Escalating the prejudice of the AGENCY's delay, Proposition 24 also  
10 eliminated the statutory safe harbor — the right of businesses to cure alleged  
11 violations before administrative enforcement. Previously, businesses could avoid  
12 penalties by addressing violations within 30 days of receiving a notice of alleged  
13 noncompliance. Proposition 24 makes a cure period wholly discretionary,  
14 meaning that the AGENCY can choose to immediately institute administrative  
15 enforcement actions. The removal of this safe harbor further underscores the  
16 importance for businesses to receive the voter mandated one year to develop,  
17 update, and implement systems to comply with the new regulations.

18       6. Though the AGENCY has blown through Proposition 24's deadlines,  
19 it has rejected requests to correspondingly adjust the date when enforcement  
20 will commence. The AGENCY's actions thus put businesses on a dramatically  
21 shortened timeline—in direct conflict with the plain language and structure of  
22 Proposition 24—with no safe harbor, resulting in prejudice unilaterally created  
23 by the AGENCY. Businesses will have far less time to reconfigure technical  
24 systems, re-engineer data flows, construct new tools, redesign websites and apps,  
25 update policies, revise contracts, train employees, and so on. These are complex,  
26 far-reaching, and arduous undertakings that require significant time and  
27 expense.

1           7.     Rushing implementation and forcing businesses to perform these  
2 tasks in a few short months or less is not what the voters intended. Proposition  
3 24 clearly mandated, and its terms specifically provided business with, a  
4 minimum one-year window between the date that a complete set of final  
5 regulations is issued and commencement of enforcement. (Civ. Code §  
6 1798.185(d).) This one-year window is necessary to provide California businesses  
7 with sufficient time to make the wide range of changes necessary to conform to  
8 the sweeping new requirements of Proposition 24 and implementing regulations.

9           8.     This Petition and Complaint therefore seeks to require the AGENCY  
10 to satisfy its statutory obligation to adopt the complete final regulations required  
11 by Proposition 24 and to toll enforcement of the law and implementing  
12 regulations until one year from the date the AGENCY adopts final regulations,  
13 as expressly required by Proposition 24. (Civ. Code §§ 1798.185(a), (d).) Such  
14 tolling is necessary to conform to the statutory requirement and voters' intent  
15 that businesses receive a one-year grace period to update their systems and  
16 processes to comply with the new legal requirements.

17           9.     In the absence of such relief, the ballot measure's plain language and  
18 will of the voters will be thwarted, and wide swaths of California's economy –  
19 each and every business with more than \$25 million in annual gross revenues –  
20 will be required to rush to design and implement complex compliance  
21 infrastructure. As a non-exhaustive set of examples, in a matter of a months or  
22 even weeks, businesses will need to rush to redesign technical infrastructure;  
23 create processes to manage the new rights of correction and sensitive data use  
24 limitations; revisit and potentially redesign consent interfaces in their websites  
25 and apps; negotiate and revise contracts with service providers, contractors, and  
26 third parties; significantly revise privacy policies and other consumer-facing  
27 documents; update websites and applications; and train employees. And that is  
28 to say nothing of some of the most complex and difficult areas for which draft

1 regulations have not even been previewed. Businesses that cannot condense a  
2 year's worth of preparation into a few short months (or less) will face exposure  
3 to administrative and civil prosecution, including significant administrative and  
4 civil fines, cease and desist orders, and injunctions.

5 10. Petitioners therefore seek:

- 6 a. A writ of mandate compelling the AGENCY to promptly adopt the  
7 final regulations referenced in Civ. Code §§ 1798.185(a)(8)-(22),  
8 as required by Proposition 24, and commanding Respondents and  
9 all other public officers acting by and through their authority to  
10 refrain from taking any steps to enforce Proposition 24 on or after  
11 July 1, 2023, until the AGENCY has adopted the required final  
12 regulations and provided businesses with the required minimum  
13 one-year grace period from final adoption to conform their  
14 practices to the new rules;
- 15 b. A declaration from this Court that the AGENCY violated its legal  
16 duty to adopt final regulations by July 1, 2022 and that  
17 Proposition 24 establishes a minimum 12-month period between  
18 the AGENCY's adoption of final implementing regulations and  
19 the AGENCY's commencement of enforcement, such that the  
20 statute and accompanying regulations cannot be enforced until  
21 12 months after the date when final regulations are adopted;
- 22 c. An injunction prohibiting Respondents, and all other public  
23 officers acting by and through their authority, from making any  
24 expenditure of public funds to enforce Proposition 24 and its  
25 accompanying regulations until 12 months after the adoption of  
26 final implementing regulations; and
- 27 d. Any other equitable or other relief deemed proper by the Court.
- 28

**PARTIES**

1  
2       11. Petitioner CALIFORNIA CHAMBER OF COMMERCE is a non-  
3 profit corporation organized under Section 501(c)(6) of the Internal Revenue  
4 Code.

5       12. Petitioner CALIFORNIA CHAMBER OF COMMERCE'S members  
6 and supporters include numerous businesses in the State of California that are  
7 subject to the requirements in the California Consumer Privacy Act of 2018  
8 ("CCPA") and Proposition 24 (the California Privacy Rights Act, or "CPRA"), as  
9 well as the regulations promulgated pursuant to those statutes. Petitioner  
10 CALIFORNIA CHAMBER OF COMMERCE, as well as a number of Petitioner's  
11 members and supporters, submitted numerous comments to the AGENCY  
12 during the course of the rulemaking process, including to request that  
13 enforcement of Proposition 24 be tolled until one year after final regulations have  
14 been issued to provide businesses with sufficient time to understand and  
15 implement the obligations established in the regulations.

16       13. Petitioner CALIFORNIA CHAMBER OF COMMERCE brings this  
17 proceeding on its own behalf and on behalf of its member businesses that are  
18 subject to Proposition 24. Petitioner CALIFORNIA CHAMBER OF  
19 COMMERCE's members would otherwise be entitled to bring this suit in their  
20 own right, the interests that Petitioner seeks to protect in this lawsuit are  
21 germane to its purpose, and neither the claims asserted, nor the relief sought  
22 herein, are unique to specific businesses and therefore do not require the  
23 participation of each and every member of Petitioner.

24       14. Many of Petitioner CALIFORNIA CHAMBER OF COMMERCE'S  
25 members are subject to Proposition 24 and will be harmed if the obligations in  
26 Proposition 24 are allowed to be enforced starting on July 1, 2023, just weeks or  
27 months after (or even before) regulations have been finally adopted and without  
28

1 providing the statutory one-year grace period necessary for those members to  
2 understand and implement their compliance obligations.

3 15. Respondent AGENCY is a new state agency created by Proposition  
4 24 to implement and enforce the 2018 CCPA and Proposition 24, the 2020 CPRA.  
5 Respondent AGENCY is empowered to conduct investigations of potential  
6 violations of the statutes and regulations within its jurisdiction, and upon  
7 determining a violation exists, to order businesses to cease and desist violations  
8 and pay administrative fines of up to \$2,500 per violation (and up to \$7,500 per  
9 violation for certain infractions). (Civ. Code §§ 1798.199.55(a), 1798.199.90(a).)  
10 Respondent AGENCY is governed by a five-member board. (*Id.* §  
11 1798.199.10(a).)

12 16. On information and belief, absent an order from this Court,  
13 Respondent AGENCY will begin enforcement of Proposition 24 on July 1, 2023,  
14 despite the fact that the necessary implementing regulations have not been  
15 published, and in any event, may or will be issued just weeks or months prior to  
16 July 1, 2023, and possibly thereafter, in contravention of the mandatory deadline  
17 and one-year implementation period established in Proposition 24. (Civ. Code §  
18 1798.185(d).)

19 17. Respondents JENNIFER M. URBAN, ALASTAIR MACTAGGART,  
20 LYDIA DE LA TORRE, and VINHCENT LE (together “Respondent BOARD  
21 MEMBERS”) are members of the governing board of the AGENCY and are sued  
22 in their official capacities only. On information and belief, absent an order from  
23 this Court, Respondent BOARD MEMBERS will cause Proposition 24 to be  
24 implemented and enforced beginning on July 1, 2023, despite the fact that the  
25 necessary implementing regulations have not been published, and in any event,  
26 may or will be issued just weeks or months prior to July 1, 2023, and possibly  
27 thereafter, in contravention of the mandatory deadline and one-year  
28 implementation period established in Proposition 24. (Civ. Code § 1798.185(d).)





1 authorizes the issuance of a writ of mandate. Section 1060 authorizes this court  
2 to issue declaratory relief. Section 526a authorizes this court to order injunctive  
3 relief.

4 21. Venue is proper under Code of Civil Procedure sections 393 and 394  
5 because the events and actions of Respondents giving rise to the claims alleged  
6 herein occurred in Sacramento County.

### 7 FACTUAL ALLEGATIONS

#### 8 **A. *The 2018 CCPA***

9 22. In 2018, the Legislature enacted the California Consumer Privacy  
10 Act of 2018 ("2018 CCPA") (Tit. 1.81.5 [commencing with Section 1798.100] of  
11 Part 4 of Div. 3 of Civ. Code). (AB 375, Stats. 2018, ch. 55.) The 2018 CCPA was  
12 the nation's first legislation to comprehensively regulate the collection and use  
13 of consumer personal data. (Assem. Com. on Privacy and Consumer Protection,  
14 Jun. 27, 2018 analysis of AB 375 (as amended Jun. 25, 2018), p. 1.)

15 23. The 2018 CCPA provided consumers with new rights regarding their  
16 personal information, including the right to know what personal information is  
17 being collected about them and whether their personal information is being sold  
18 and to whom; the right to access their personal information; the right to delete  
19 personal information collected from them; the right to opt-out or opt-in to the  
20 sale of their personal information, depending on age of the consumer; and the  
21 right to equal service and price, even if they exercise such rights. (AB 375, Stats.  
22 2018, ch. 55.) These rights are currently in effect and are being enforced.

23 24. The 2018 CCPA assigned administrative oversight and  
24 implementation to Respondent ATTORNEY GENERAL, including the  
25 responsibility for adopting implementing regulations. (AB 375; Civ. Code §  
26 1798.185.) The 2018 CCPA provided express direction to the ATTORNEY  
27 GENERAL to promulgate regulations on seven specific matters and provided  
28

1 catch-all authority to the ATTORNEY GENERAL to adopt regulations “as  
2 necessary” to further the purposes of the Act. (Civ. Code §§ 1798.185(a)-(b).)

3 ***B. Proposition 24 Significantly Broadens the 2018 CCPA.***

4 25. In November 2020, California voters approved Proposition 24, the  
5 California Privacy Rights Act of 2020 (the “2020 CPRA”). The 2020 CPRA  
6 amended 18 of the 21 statutory sections CCPA originally created and added 21  
7 new statutory sections to Title 1.81.5.

8 26. Overall, the law makes sweeping changes to materially expand the  
9 scope of the 2018 CCPA in various respects. To name some examples:

- 10
- 11 a. It imposes new requirements for businesses to protect personal  
12 information, including by minimizing data collection, limiting  
13 data retention, and protecting data security. It also extends  
14 various requirements in the 2018 CCPA to the sharing of  
15 personal information, not just the sale of such data. (See, e.g., Civ.  
16 Code §§ 1798.110, 1798.115, 1798.120, 1798.135.)
- 17 b. It adds three new substantive consumer privacy rights: (1)  
18 consumers may opt-out of the “sharing” of personal information;  
19 (2) consumers can direct businesses to correct personal  
20 information that they possess; and (3) consumers can direct  
21 businesses to limit their use and disclosure of “sensitive” personal  
22 information, a novel category not contained in the 2018 CCPA.  
23 (Civ. Code § 1798.106, 1798.120, 1798.121, 1798.140(ae).)
- 24 c. It requires businesses to notify and work with contractors, service  
25 providers, and any third parties to whom the business has sold or  
26 shared personal information to implement consumer requests  
27 regarding personal information. (Civ. Code §§ 1798.105,  
28 1798.100(d) [requiring agreements with such entities that  
contain specified terms], 1798.121, 1798.130(a)(3)(A).) It also  
requires new provisions to be included in contracts with service  
providers, contractors, and third parties. (See, e.g., Civ. Code §§  
1798.100(d), 1798.140(ag).)
- d. It expands the temporal scope of data covered by requests for a  
copy of personal information collected, sold, or shared. (Civ. Code

1 §§ 1798.110(b), 1798.130(a)(3), 1798.115(b), 1798.130(a)(4)(B.)

2 e. It amends the penalty and enforcement provisions in the 2018  
3 CCPA by adopting a new \$7,500 penalty for each violation of the  
4 title involving the personal information of a minor (Civ. Code §  
5 1798.199.90) and repealing mitigation provisions in the 2018  
6 CCPA that allowed businesses to avoid penalties by addressing  
7 alleged violations within 30 days of receiving a notice of alleged  
8 noncompliance (Civ. Code § 1798.155 [no longer containing the  
9 cure period that was in the 2018 CCPA].).

10 27. In addition, the 2020 CPRA introduced many new requirements that  
11 are not spelled out in the statute, but are instead left to regulatory rulemaking.  
12 Those include rules about performing cybersecurity audits on an annual basis;  
13 conducting risk assessments about the processing of personal information; and  
14 the use of “automated decision-making technology.” (Civ. Code §§  
15 1798.185(a)(15), (16).)

16 28. In addition, the 2020 CPRA created the AGENCY and transferred  
17 regulatory authority from the ATTORNEY GENERAL to the AGENCY. (Civ.  
18 Code § 1798.185(d).) In connection with the AGENCY’s rulemaking duties, the  
19 2020 CPRA expressly required the AGENCY to adopt a full set of regulations on  
20 15 new subjects,<sup>1</sup> stating that the “timeline for adopting final regulations  
21 required by the act adding this subdivision shall be July 1, 2022.” (Civ. Code §  
22 1798.185(d).) The AGENCY has expressly acknowledged that these regulations  
23 are legally required and integral to “operationaliz[ing] new rights and concepts  
24 introduced by the CPRA” and to providing the “clarity and specificity [necessary]  
25 to implement the law.” (Pet. Ex. 2.)

26 29. To name just a few examples:

27 a. The AGENCY must establish by regulation how often and under

28 <sup>1</sup> The 2018 CCPA required regulations on seven subjects, and the 2020 CPRA requires regulations on fifteen additional subjects. (Civ. Code §§ 1798.185(a)(1)-(22).)

1 what circumstances a consumer may request correction of  
2 personal information, how a business is required to respond, and  
3 what businesses can do to resolve concerns regarding the  
4 accuracy of information and to prevent fraud. (Civ. Code §  
1798.185(a)(8).)

5 b. The AGENCY must define standards such as “impossibility” and  
6 “disproportionate effort” that establish guardrails regarding the  
7 extent of efforts businesses must expend to implement certain  
8 customer requests. (*Id.* § 1798.185(a)(9).)

9 c. The AGENCY must issue regulations regarding what constitutes  
10 a “dark pattern”—i.e., design elements in interfaces that cannot  
11 be used to gain consumer consent because they are deemed  
12 manipulative. (*Id.* § 1798.185(a)(20).)

13 d. The AGENCY must define what constitutes the processing of  
14 personal information for a “business purpose,” a critical threshold  
15 concept that governs the scope of numerous business obligations  
16 regarding personal information. (Civ. Code §§ 1798.185(a)(9)-  
17 (10), 1798.135(f), 1798.140(ag).)

18 e. The AGENCY must establish requirements and technical  
19 specifications for an “opt-out preference signal” to indicate a  
20 consumer’s intent to restrict the sale, sharing, use, or disclosure  
21 of personal information and to limit the use or disclosure of the  
22 consumer’s sensitive personal information. (See Civ. Code §§  
23 1798.185(a)(19), 1798.120.)

24 f. The AGENCY must establish rules related to cybersecurity  
25 audits, risk assessments, and automated decision-making  
26 technologies, regulatory categories left entirely to the Agency,  
27 with no substantive rules included in the actual statute. (See Civ.  
28 Code §§ 1798.185(a)(15), (16).)

**C. *The 2020 CPRA Deliberately Sets the Deadline for Final  
Rulemaking and the Start of Enforcement One Year Apart.***

30. Proposition 24 explicitly mandates that the AGENCY adopt  
regulations addressing *all* of the 15 new topics listed in subsection  
1798.185(a)(8)-(22) no later than July 1, 2022. Specifically, the statute provides

1 that that the “timeline for adopting final regulations *required by the act*  
2 *adding this subdivision* [i.e., Prop. 24] *shall be July 1, 2022.*” (Civ. Code §  
3 1798.185(d), emphasis added; see also Pet. Ex. 3, Written Justification for  
4 Earlier Effective Date [“The CPRA *requires* the Agency to adopt regulations to  
5 operationalize the CPRA amendments to the CCPA by *July 1, 2022*], emphasis  
6 added; Pet. Ex. 2 [“The Agency is directed to adopt regulations to further the  
7 purposes of the Act”].)

8 31. This is a mandatory instruction, as the statutory scheme makes  
9 clear. Subdivision (a) of section 1798.185 lists the regulations that “shall” be  
10 adopted, which includes the list of 15 separate substantive areas newly added by  
11 the 2020 CPRA. Subsection (b) of section 1798.185 lists additional regulations  
12 that “may” be adopted, which are those “necessary to further the purposes of this  
13 title.” (Civ. Code §§ 1798.185(a), (b).) The July 1, 2022, deadline is tied to  
14 regulations “required by the Act.” (*Id.* § 1798.185(d).) The regulations that are  
15 “required” are those set forth in subdivision (a)—the ones the Agency “shall”  
16 adopt. Thus, it is clearly obligatory for the Agency to promulgate the full set of  
17 1798.185(a)(8)-(22) regulations by July 1, 2022. (See *De Leon v. Juanita’s Foods*  
18 (2022) 85 Cal.App.5th 740, 752 [30-day statutory deadline for payment of  
19 arbitration fees is “clear and unambiguous”].)

20 32. Particularly telling is that the voters used both “shall” and “may” in  
21 the same provision to signify which administrative actions are obligatory and  
22 which are discretionary. (See *Common Cause v. Bd. of Supervisors* (1989) 49  
23 Cal.3d 432, 443 [“it is a well-settled principle of statutory construction that the  
24 word ‘may’ is ordinarily construed as permissive, whereas ‘shall’ is ordinarily  
25 construed as mandatory”]; *City of Grass Valley v. Cohen* (2017) 17 Cal.App.5th  
26 567, 577 [“The use of ‘may’ and ‘shall’ in the same statutory provision is  
27 illuminating.”]; *Atkinson v. Elk Corp. of Tex.* (2006) 142 Cal.App.4th 212, 228.)

1 The Agency had a mandatory duty to adopt all of the subdivision (a)(8)-(22)  
2 regulations by July 1, 2022.

3 33. And if there were any ambiguity about this mandatory obligation  
4 (there is not), the drafters of Proposition 24 eliminated it by expressly stating  
5 that “final regulations implementing the new provisions of the CPRA *have to be*  
6 *adopted*” by July 1, 2022. (Californians for Consumer Privacy, *CPRA Timeline*,  
7 <https://www.caprivacy.org/cpra-timeline/> [Prop. 24 proponents’ ballot measure  
8 committee statement].)

9 34. The law is equally clear that the voters did not intend for Proposition  
10 24 to be enforced until the Agency issued the full set of final regulations *and*  
11 businesses received a one-year grace period to conform their operations and  
12 practices with those new statutory and regulatory requirements. In the very  
13 same provision (entitled “Regulations”), the voters specified that businesses  
14 would have *at least* one year to make conforming changes based on the text of  
15 the final regulations, prior to any Agency enforcement. The statute states:  
16 “Notwithstanding any other law, civil and administrative enforcement of the  
17 provisions of law added or amended by this act ***shall not commence*** until July  
18 1, 2023 [i.e., one year after the AGENCY’s mandatory deadline for issuing final  
19 regulations], and shall only apply to violations occurring on or after that date.”  
20 (Civ. Code § 1798.185(d), emphasis added.)

21 35. This one-year implementation period is an essential feature of  
22 Proposition 24. The Proposition significantly revised the 2018 CCPA and left  
23 numerous critical details to be addressed through a complete set of regulations,  
24 as explained above. The voters therefore established a detailed, orderly, and  
25 phased implementation and enforcement timetable. Under this framework,  
26 development of the implementing regulations would commence immediately  
27 (Prop. 24, § 31(b)), final regulations would be issued no later than July 1, 2022  
28 (Civ. Code § 1798.185(d)), the law would be operative on January 1, 2023, and

1 enforcement would begin no earlier than July 1, 2023. (Prop. 24, §§ 31(a)-(b); Civ.  
2 Code § 1798.185(d).) The plain text thus establishes a timeline with two inter-  
3 related steps: (1) the Agency would adopt a complete set of final regulations no  
4 later than July 1, 2022; and (2) the Agency would begin enforcement no earlier  
5 than one year later, July 1, 2023.

6 36. The voters' intent that businesses have sufficient time to implement  
7 the new requirements in an orderly way is corroborated by the law's findings,  
8 declarations, and purpose sections. The voters explained that one of the primary  
9 purposes of law's orderly implementation provisions was to "strengthen[]  
10 consumer privacy *while giving attention to the impact on business and*  
11 *innovation.*" (Prop. 24 § 3(C)(1), emphasis added; *see also id.* §§ 3(C)(2), 3(C)(4).)

12 37. Altogether lacking from these or any other component of Proposition  
13 24, including the legislative history, is any statement indicating that the Agency  
14 can issue mandatory regulations in a piecemeal format, or miss its own deadlines  
15 but hold others against businesses. The AGENCY's disregard for the statutory  
16 deadlines and scheme is incompatible with the deliberate effort in Proposition  
17 24 to provide businesses with a one-year grace period to make the updates  
18 needed to comply with a new and complete set of complex legal requirements.

19 38. Even if businesses wanted to complete these updates before July 1,  
20 2023, they could not do so absent final regulations. Proposition 24 does not alone  
21 give businesses sufficient guidance to know what is required by the law. The  
22 statutory provisions are too skeletal and indefinite to give businesses reasonably  
23 fair notice of what is expected of them and how they can achieve compliance.  
24 This is evident from the long list of required regulations in Section 1798.185(a),  
25 the 66 pages of detailed regulations that the Agency has proposed (see Pet. Ex.  
26 4), and the extensive comments provided during the rulemaking process. The  
27 voters themselves understood this to be the case and architected Proposition 24  
28 accordingly; they mandated the issuance of a series of highly substantive



1 regulations by a date certain and extended enforcement a minimum of one year  
2 into the future.

3 39. Two examples illuminate the Act's vagueness and the critical need  
4 for gap-filling regulations. First, the entire scope of the consumer's statutory  
5 "right to correct" information consists of three very general paragraphs that  
6 provide that: (1) consumers "shall have the right to request" that a business  
7 correct inaccurate information; (2) businesses "shall disclose" that consumers  
8 have a right to request corrections; and (3) businesses that receive such requests  
9 "shall use commercially reasonable efforts" to correct inaccuracies. (Civ. Code §  
10 1798.106.) Entirely lacking are any standards or criteria for a business to  
11 determine how, for example, to discern which requests are credible, how to  
12 authenticate the identity of the requester, how quickly requests must be  
13 processed, how to determine the accuracy of information subject to a request,  
14 how to communicate determinations with consumers, whether the business has  
15 obligations to work with service providers and contractors when it does  
16 determine that information is inaccurate, how often a business must assess  
17 repeat requests for correction, and numerous other details that are critical to  
18 enabling a business to conform to the new legal requirement. Tellingly, the draft  
19 regulations submitted in February—which have not yet been published—spend  
20 four single-spaced pages providing proposed answers to these and  
21 numerous other questions that are left unanswered by the statutory text. (See  
22 11 C.C.R. § 7023 [explaining, for instance, some of the various factors that a  
23 business should consider in its totality of the circumstances analysis of whether  
24 information is accurate].)

25 40. Second, the brief language in Proposition 24 establishing a  
26 consumer's right to direct a business to limit its use of sensitive personal  
27 information leaves numerous weighty questions unaddressed. (Civ. Code §  
28 1798.121 [businesses that have received such requests may only use personal

1 information for limited purposes].) These include the interface a business must  
2 provide to enable a consumer to submit a request, whether a business must (or  
3 can) verify the identity of the requester and what to do if the request is  
4 fraudulent, how quickly a business must fulfill a request, whether a business  
5 must (or can) communicate with service providers and contractors about the  
6 request, whether a business must notify the consumer that it has fulfilled the  
7 request (and, if required, what to do to satisfy this requirement), and when a  
8 business can use sensitive personal information without being required to offer  
9 consumers a right to limit this use. These and numerous other questions are  
10 addressed in another nearly four pages of single-spaced regulatory text in the  
11 draft regulations published in February—which were nearly eight months late  
12 and still are not published. (See 11 C.C.R. § 7027.)

13 41. These are just two of the numerous significant requirements in  
14 Proposition 24 that cannot be implemented or enforced with any degree of  
15 certainty or consistency in the absence of detailed regulations. (*Compare* Civ.  
16 Code § 1798.135 [opt-out preference signals], *with* 11 C.C.R. § 7025; *compare* Civ.  
17 Code § 1798.140(l) [brief definition of “dark pattern” interface], *with* 11 C.C.R. §  
18 7004 [extensive standards for interfaces for CCPA requests and requests to  
19 obtain consumer consent that must be followed to avoid a dark pattern]; *compare*  
20 Civ. Code §§ 1798.105, 1798.130 [exemptions from requirement to delete or  
21 disclose information if doing so would require “disproportionate effort”], *with* 11  
22 C.C.R. § 7001(j) [detailed definition of key term]; *compare* Civ. Code §§  
23 1798.140(j)(1), 1798.140(ai) [definitions of “contractor” and “third parties”], *with*  
24 11 C.C.R. §§ 7051, 7053 [detailed requirements for contracts with service  
25 providers, contractors, and third parties].)

1           ***D. The AGENCY Still Has Not Published Any Final Regulations***  
2           ***and Has Not Even Started Work on Numerous Other,***  
3           ***Required Regulations.***

4           42. Despite the statute's express deadline for issuing the required  
5 regulations, the AGENCY still has not published a single final regulation. It was  
6 not until July 8, 2022—one week *after* the deadline for adoption of final  
7 regulations—that the AGENCY published its first Notice of Proposed  
8 Rulemaking, Initial Statement of Reasons, and text of Proposed Regulations.  
9 (Pet. Ex. 2.) That first set of belated draft regulations was piecemeal and  
10 incomplete; it only addressed 8 of the 15 new topics listed in Section 1798.185(a).

11           43. In response to that partial draft set of regulations, the AGENCY  
12 received more than 100 written comments, many of them thorough, detailed, and  
13 technical. On November 3, 2022, the Agency issued a modified text of Proposed  
14 Regulations, containing a variety of substantive revisions to the July 8, 2022,  
15 draft. This revised set of partial proposed regulations led to another round of  
16 over 50 detailed comments.

17           44. On February 3, 2023, the AGENCY's Board approved the revised set  
18 of Proposed Regulations, and on February 14, 2023, the AGENCY submitted the  
19 rulemaking package with that partial set of proposed regulations to the Office of  
20 Administrative Law for final review (the "February Draft Regulations"). The  
21 February Draft Regulations cover 66 pages and contain 41 separate sections that  
22 will require businesses to undertake extensive substantive changes to their  
23 practices and policies. (Pet. Ex. 4.) These include overhauling privacy policies,  
24 establishing an entirely new framework for handling sensitive personal  
25 information, establishing procedures to track and timely communicate with  
26 third parties with whom personal information is shared, renegotiating contracts  
27 to ensure compliance, and implementing extensive new procedures to receive  
28 and process consumer requests to correct personal information. (11 C.C.R. §§  
7014, 7023, 7024(h)-(i), 7027, 7050-7053.)

1           45. The AGENCY is not only woefully late on these February Draft  
2 Regulations, but it concedes (as it must) that they are materially incomplete.  
3 Though the statute called for a full set of regulations on 15 new topics, both the  
4 Notice of Proposed Rulemaking and Initial Statement of Reasons state that the  
5 February Draft Regulations only cover the topics contained in paragraphs (8)-  
6 (11), (18)-(20), and (22) of Civil Code section 1798.185(a). (See Pet. Ex. 2.) In  
7 other words, the February Draft Regulations address only eight of the fifteen  
8 new regulatory topics specified in Proposition 24. This piecemeal approach is  
9 incompatible with the mandatory language of the 2020 CPRA requiring the  
10 Agency to issue “final regulations” regarding *all* fifteen substantive areas by July  
11 1, 2022. (Civ. Code §§ 1798.185(a), (d).)

12           46. The Agency has not published even draft regulations addressing  
13 some of the most novel and complicated topics mandated by the law’s rulemaking  
14 provision. The Notice of Proposed Rulemaking expressly acknowledges that  
15 “[t]he Agency will not be promulgating rules on cybersecurity audits (§  
16 1798.185(a)(15)(A)), risk assessments, (§ 1798.185(a)(15)(B)), or automated  
17 decision-making technology (§ 1798.185(a)(16)) at this time.” (Pet. Ex. 2.)

18           47. The absence of final, clarifying regulations on these and other topics  
19 will leave countless businesses guessing at the concrete actions they will need to  
20 undertake to conform to the law.

21           ***E. The February Draft Regulations, Proposed Nearly Eight***  
22           ***Months Late, Make Numerous Substantive Changes to the***  
23           ***Obligations of Petitioners and Other Businesses and Are***  
24           ***Incomplete.***

25           48. The February Draft Regulations are lengthy and impose a complex  
26 set of requirements on businesses. (See Pet. Ex. 4.) Many of those requirements  
27 are net new, meaning they appear in the regulations but not the underlying  
28 statute. (See ¶¶ 38-42, *supra*.) As a result, once adopted, businesses will need to

1 make significant and substantive changes to their operations to comply with the  
2 regulations.

3 49. In addition, as noted above, there are key provisions that have not  
4 yet even been proposed, which leaves countless businesses guessing at the  
5 concrete actions they will need to undertake and whether they are even subject  
6 to certain requirements. For example, the statute mandates that businesses  
7 whose processing of personal information presents “significant risk” to  
8 consumers’ “privacy or security” perform an annual cybersecurity audit and  
9 submit to the Agency “on a regular basis” a risk assessment. (Civ. Code §  
10 1798.185(a)(15).) But the law does not define when a business’s processing of  
11 personal information presents “significant risk” to consumer privacy or security,  
12 nor does it provide any actionable information about the required scope of the  
13 audit, the procedures necessary to ensure it is “thorough and independent,” the  
14 frequency of the risk assessment, or how a business should conduct the  
15 mandatory process of “weighing the benefits resulting from the processing” of  
16 personal information against “the potential risks to the rights of the consumer  
17 associated with that processing.” (*Id.* §§ 1798.185(a)(15)(A), (B).)

18 50. Likewise, businesses have been provided with no information about  
19 their obligations when utilizing “automated decision-making technology.” (Civ.  
20 Code § 1798.185(a)(16).) The statute does not even define the term. Instead, it  
21 leaves to the AGENCY to “[i]ssu[e] regulations governing access and opt-out  
22 rights with respect to businesses’ use of automated decision-making technology,  
23 including profiling and requiring businesses’ response to access requests to  
24 include meaningful information about the logic involved in such decision-making  
25 processes, as well as a description of the likely outcome of the process with  
26 respect to the consumer.” (*Id.*) Businesses have no way to prepare today for  
27 whatever these rules may require. Changes to internal machine processes, as  
28 well as requirements to explain the logic of such processes, could be an intensely

1 burdensome operational process that may easily require at least a full year to  
2 implement.

3 ***F. The AGENCY's Delays Violate the Law and Have Prevented***  
4 ***Businesses from Understanding their Legal Obligations.***

5 51. The AGENCY's eight-month delay in issuing final regulations,  
6 combined with the complexity and number of issues involved, have prompted a  
7 wide swath of businesses and other interested parties to call on the AGENCY to  
8 toll enforcement of the law, in line with the text of Proposition 24. Together, the  
9 AGENCY received 27 written comments and 10 oral comments (including  
10 comments from Petitioner California Chamber of Commerce) requesting  
11 preservation of the time sequencing set forth in Proposition 24 to give businesses  
12 sufficient time to make conforming changes to comply with the law.

13 52. The AGENCY, however, has failed to heed these requests, reasoning  
14 that businesses had been aware of the "general contours" of the *proposed*  
15 regulations and that any deferral of enforcement would be less "effective in  
16 carrying out the purpose and intent of the CCPA than having the regulations  
17 take effect in accordance with the standard rules governing rulemaking"  
18 contained in the Administrative Procedure Act. (Pet. Ex. 5.) The AGENCY stated  
19 only, and without elaboration, that it "*may* consider the effect that the delay in  
20 adopting the regulations has had on a business' ability to comply." (*Id.*, emphasis  
21 added.)

22 53. This is both unhelpful and cold comfort for businesses. First, the  
23 draft regulations have been evolving over time, and their uncertain draft state  
24 fails to provide businesses with the certainty necessary to make conforming  
25 changes. Businesses want to comply with the law, but before undertaking  
26 technical changes, revising contracts, updating policies, and so on, they need to  
27 know what the law actually requires. That is still not yet clear because no final  
28 regulations have been adopted to date. Second, the AGENCY's statement that it

1 “may” consider its own delay in an enforcement action is purely discretionary.  
2 The AGENCY can still enforce immediately on July 1, 2023, if it so chooses, and  
3 businesses, with scarce time to prepare and no mandatory safe harbor cure  
4 period, will have little protection against potential regulatory actions carrying  
5 penalties of up to \$2,500 to \$7,500 for each violation, as well as cease and desist  
6 orders and injunctions. (Civ. Code §§ 1798.155, 1798.199.90, 1798.199.95).)

7 54. This situation is manifestly unfair, as it penalizes businesses for the  
8 AGENCY's own tardiness in issuing mandatory regulations. Moreover, it plainly  
9 violates the will of voters who enacted Proposition 24. Voters clearly intended to  
10 give businesses a full year to comply with a complete set of mandatory  
11 regulations. The AGENCY has ignored its statutory deadline and the  
12 requirement to promulgate a complete set of regulations. Petitioners seek a  
13 reasonable tolling of any efforts to enforce Proposition 24 and implementing  
14 regulations until at least one year after final regulations have been adopted,  
15 thereby providing businesses with the one year the voters originally intended to  
16 come into compliance with numerous, substantive, new legal requirements.

17 **FIRST CAUSE OF ACTION**

18 **Writ of Mandate – Code of Civil Procedure §§ 1085 and 1086**

19 55. Petitioners reallege and incorporate by reference Paragraphs 1  
20 through 54 above, as if fully set forth herein.

21 56. Petitioners are beneficially interested in the issuance of a writ as  
22 requested and have no plain, speedy, or adequate remedy at law as to all causes  
23 of action set forth herein.

24 57. A writ of mandate is necessary commanding that Respondents and  
25 all other public officers acting by and through their authority refrain from  
26 enforcing Proposition 24 and implementing regulations until 12 months after  
27 adoption of final implementing regulations because Respondents' failure to  
28 perform their mandatory duty to timely promulgate implementing regulations

1 creates a clear, present, and impermissible conflict with the statutory scheme  
2 enacted by the voters. Respondents' failure to perform their mandatory duties  
3 also prejudices and deprives businesses of the statutorily required one-year  
4 timeframe to enable them to comply with the statute and regulations in  
5 contravention of the intent of the voters.<sup>2</sup>

6 58. A writ of mandate is also necessary commanding that Respondent  
7 AGENCY and Respondent BOARD MEMBERS promptly adopt the final  
8 regulations required by Proposition 24.

9 **SECOND CAUSE OF ACTION**

10 **Declaratory Relief – Code of Civil Procedure §§ 1060 and 1062**

11 59. Petitioners reallege and incorporate by reference Paragraphs 1  
12 through 58 above, as if fully set forth herein.

13 60. Proposition 24 required that regulations for its implementation be  
14 promulgated by July 1, 2022, precisely 12 months before the measure would  
15 become fully operative and enforceable by the AGENCY. As of March 30, 2023,  
16 the regulations have not been published in final form. In fact, as of this date, the  
17 AGENCY has not even issued initial draft regulations with respect to at least  
18 three substantive requirements imposed by Proposition 24. These delays and  
19 failures to satisfy the obligations of Proposition 24 leave businesses in the  
20 untenable position of needing to guess at the concrete steps they will need to  
21

---

22 <sup>2</sup> For clarity, the one-year tolling and prohibition of enforcement should apply to all  
23 regulations required under Section 1798.185(a)(8)-(22), and the one-year time period  
24 should run separately from the adoption date of each required regulation. For example,  
25 if some regulations are adopted in April 2023 and others in September 2023, then  
26 businesses should be afforded the same amount of time to come into compliance with  
27 the regulations that were adopted in September 2023 as the regulations that were  
28 adopted in April 2023. The statute clearly contemplated a complete set of regulations  
by July 1, 2022, and the Agency's decision to proceed in a piecemeal approach should  
not be held against businesses. The only way to preserve the statutory framework is to  
give businesses a full year grace period running from whenever each regulation is  
adopted.



1 take to bring their operations into compliance with the law. In addition to  
2 requiring businesses to move to chaotically implement a wide range of new  
3 practices, Respondent BOARD MEMBERS' and AGENCY's failure to timely  
4 perform their duty under Civil Code section 1798.185(d) will expose Petitioners  
5 and numerous other businesses to civil prosecution and punishment.

6 61. An actual controversy has arisen and now exists between Petitioners  
7 and Respondents as to whether Proposition 24 is enforceable as of July 1, 2023,  
8 in the absence of implementing regulations and the observance of the one-year  
9 implementation grace period, both of which are required by Civil Code section  
10 1798.185(d).

11 62. Petitioners are informed and believe that Respondents will begin to  
12 enforce Proposition 24 starting on July 1, 2023, despite Petitioners' and others'  
13 repeated requests for an adjustment to the enforcement deadline, unless  
14 restrained from doing so by a court of law.

15 63. Petitioners therefore seek a declaration pursuant to Code of Civil  
16 Procedure sections 1060 and 1062 that the Respondents AGENCY and BOARD  
17 MEMBERS had a legal duty to adopt final regulations by July 1, 2022, and that  
18 Proposition 24 establishes a minimum 12-month period between adoption of  
19 final implementing regulations and commencement of enforcement.

20 64. Petitioners further seek a declaration from this Court that  
21 businesses are not subject to enforcement on July 1, 2023, given the AGENCY's  
22 failure to timely adopt regulations consistent with the text of the statute.

23 65. Petitioners further seek a declaration pursuant to Code of Civil  
24 Procedure section 1060 that, pursuant to the foregoing, any actions taken by  
25 Respondents and Does 1-100 to enforce Proposition 24 and implementing  
26 regulations before, on, or after July 1, 2023, are improper and shall have no force  
27 or effect until one year has passed after the date on which final regulations are  
28 adopted.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**THIRD CAUSE OF ACTION**

**Injunctive Relief**

**Code of Civil Procedure § 526a**

66. Petitioners reallege and incorporate by reference Paragraphs 1 through 65 above, as if fully set forth herein.

67. Respondent AGENCY and Respondent BOARD MEMBERS are disregarding the statutory requirements of Proposition 24. Petitioners lack an adequate remedy at law and injunctive relief is necessary to prevent the illegal expenditure and/or waste of public funds.

68. Further exacerbating the potential illegal expenditure and/or waste of public funds is the fact that California consumers currently enjoy significant privacy protections through the 2018 CCPA and other laws, such that the public interest in privacy is already being protected.

**PRAYER**

WHEREFORE, Petitioners pray that this Court:

1. Issue a peremptory writ of mandate commanding Respondents AGENCY and Board Members to promptly adopt the final regulations required by Proposition 24 and commanding Respondents and all other public officers acting by and through their authority to refrain from taking any steps to enforce Proposition 24 and implementing regulations on or after July 1, 2023, until the AGENCY has adopted the required final regulations in Section 1798.185(a) and provided businesses with the required minimum one-year grace period from the date each regulation is adopted.

2. Issue a declaratory judgment that Section 1798.185(d) of the Civil Code imposes a legal duty on Respondent AGENCY and Respondent BOARD MEMBERS to issue the complete set of final regulations, as detailed in Section 1798.185(a)(8)-(22), no later than July 1, 2022, and establishes that the statute

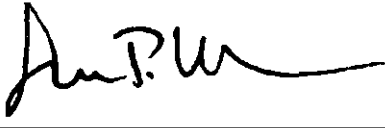
1 and implementing regulations cannot be enforced until 12 months after the date  
2 when each regulation is adopted.

3 3. Enjoin Respondents and all other public officers acting by and  
4 through their authority from making any expenditure of public funds enforce  
5 Proposition 24 and implementing regulations on or after July 1, 2023, until 12  
6 months after the date each of the regulations is adopted.

7 4. Grant such other and further relief as it deems necessary and  
8 appropriate.

9  
10 Dated: March 30, 2023

Respectfully submitted,  
NIELSEN MERKSAMER  
PARRINELLO GROSS & LEONI LLP

11  
12  
13 By:   
14 Sean P. Welch  
15 Kurt R. Oneto  
16 David J. Lazarus  
17 *Attorneys for Petitioner*  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**VERIFICATION**

I, Gretel Tortolani, declare as follows:

I am the Executive Vice President and Chief Financial Officer for Petitioner California Chamber of Commerce in the above-captioned case. I have read the foregoing Petition for Writ of Mandate and Complaint for Declaratory and Injunctive Relief and know the contents thereof. The facts state therein are true and within my personal knowledge, except those matters which are alleged upon information and belief, and as to those matters, I believe them to be true.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed on March 29, 2023, at Sacramento, California.



Gretel Tortolani

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

*Exhibit 1*

application not declared invalid or unconstitutional without regard to whether any portion of this act or application thereof would be subsequently declared invalid.

**PROPOSITION 24**

This initiative measure is submitted to the people in accordance with the provisions of Section 8 of Article II of the California Constitution.

This initiative measure amends and adds sections to the Civil Code; therefore, existing provisions proposed to be deleted are printed in ~~strikeout type~~ and new provisions proposed to be added are printed in *italic type* to indicate that they are new.

**PROPOSED LAW**

The California Privacy Rights Act of 2020

SECTION 0.5: Table of Contents

Section 1: Title: The California Privacy Rights Act of 2020

Section 2: Findings and Declarations

Section 3: Purpose and Intent

- A. Consumer Rights
- B. Responsibilities of Businesses
- C. Implementation of the Law

Section 4: General Duties of Businesses that Collect Personal Information

Section 5: Consumers' Right to Delete Personal Information

Section 6: Consumers' Right to Correct Inaccurate Personal Information

Section 7: Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information

Section 8: Consumers' Right to Know What Personal Information is Sold or Shared and to Whom

Section 9: Consumers' Right to Opt Out of Sale or Sharing of Personal Information

Section 10: Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information

Section 11: Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights

Section 12: Notice, Disclosure, Correction, and Deletion Requirements

Section 13: Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information

Section 14: Definitions

Section 15: Exemptions

Section 16: Personal Information Security Breaches

Section 17: Administrative Enforcement

Section 18: Consumer Privacy Fund

Section 19: Conflicting Provisions

Section 20: Preemption

Section 21: Regulations

Section 22: Anti-Avoidance

Section 23: Waiver

Section 24: Establishment of California Privacy Protection Agency

Section 25: Amendment

Section 26: Severability

Section 27: Conflicting Initiatives

Section 28: Standing

Section 29: Construction

Section 30: Savings Clause

Section 31: Effective and Operative Dates

SEC. 1. Title.

This measure shall be known, and may be cited, as the "California Privacy Rights Act of 2020."

SEC. 2. Findings and Declarations.

The people of the State of California hereby find and declare all of the following:

A. In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. Voters acted in response to the accelerating encroachment on personal freedom and security caused by increased data collection and usage in contemporary society. The amendment established a legal and enforceable constitutional right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information.

B. Since California voters approved the constitutional right of privacy, the California Legislature has adopted specific mechanisms to safeguard Californians' privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, but consumers had no right to learn what personal information a business had collected about them and how they used it or to direct businesses not to sell the consumer's personal information.

C. That changed in 2018, when more than 629,000 California voters signed petitions to qualify the California Consumer Privacy Act of 2018 for the ballot. In response to the measure's qualification, the Legislature enacted the California Consumer Privacy Act of 2018 (CCPA) into law. The CCPA gives California consumers the right to learn what information a business has collected about them, to delete their personal information, to stop businesses

23

24

from selling their personal information, including using it to target them with ads that follow them as they browse the internet from one website to another, and to hold businesses accountable if they do not take reasonable steps to safeguard their personal information.

D. Even before the CCPA had gone into effect, the Legislature considered many bills in 2019 to amend the law, some of which would have significantly weakened it. Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation.

E. Rather than diluting privacy rights, California should strengthen them over time. Many businesses collect and use consumers' personal information, sometimes without consumers' knowledge regarding the business' use and retention of their personal information. In practice, consumers are often entering into a form of contractual arrangement in which, while they do not pay money for a good or service, they exchange access to that good or service in return for access to their attention or access to their personal information. Because the value of the personal information they are exchanging for the good or service is often opaque, depending on the practices of the business, consumers often have no good way to value the transaction. In addition, the terms of agreement or policies in which the arrangements are spelled out, are often complex and unclear, and as a result, most consumers never have the time to read or understand them.

F. This asymmetry of information makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses. Unlike in other areas of the economy where consumers can comparison shop, or can understand at a glance if a good or service is expensive or affordable, it is hard for the consumer to know how much the consumer's information is worth to any given business when data use practices vary so widely between businesses.

G. The state therefore has an interest in mandating laws that will allow consumers to understand more fully how their information is being used and for what purposes. In the same way that ingredient labels on foods help consumers shop more effectively, disclosure around data management practices will help consumers become more informed counterparties in the data economy and promote competition. Additionally, if a consumer can tell a business not to sell the consumer's data, then that consumer will not have to scour a privacy policy to see whether the business is, in fact, selling that data, and the resulting savings in time is worth, in the aggregate, a tremendous amount of money.

H. Consumers need stronger laws to place them on a more equal footing when negotiating with businesses in order to protect their rights. Consumers should be entitled to a clear explanation of the uses of their

personal information, including how it is used for advertising, and to control, correct, or delete it, including by allowing consumers to limit businesses' use of their sensitive personal information to help guard against identity theft, to opt-out of the sale and sharing of their personal information, and to request that businesses correct inaccurate information about them.

I. California is the world leader in many new technologies that have reshaped our society. The world today is unimaginable without the internet, one of the most momentous inventions in human history, and the new services and businesses that arose on top of it, many of which were invented here in California. One of the most successful business models for the internet has been services that rely on advertising to make money as opposed to charging consumers a fee. Advertising-supported services have existed for generations and can be a great model for consumers and businesses alike. However, some advertising businesses today use technologies and tools that are opaque to consumers to collect and trade vast amounts of personal information, to track them across the internet, and to create detailed profiles of their individual interests. Some companies that do not charge consumers a fee, subsidize these services by monetizing consumers' personal information. Consumers should have the information and tools necessary to limit the use of their information to noninvasive proprivacy advertising, where their personal information is not sold to or shared with hundreds of businesses they've never heard of, if they choose to do so. Absent these tools, it will be virtually impossible for consumers to fully understand these contracts they are essentially entering into when they interact with various businesses.

J. Children are particularly vulnerable from a negotiating perspective with respect to their privacy rights. Parents should be able to control what information is collected and sold or shared about their young children and should be given the right to demand that companies erase information collected about their children.

K. Business should also be held directly accountable to consumers for data security breaches and notify consumers when their most sensitive information has been compromised.

L. An independent watchdog whose mission is to protect consumer privacy should ensure that businesses and consumers are well-informed about their rights and obligations and should vigorously enforce the law against businesses that violate consumers' privacy rights.

SEC. 3. Purpose and Intent.

In enacting this act, it is the purpose and intent of the people of the State of California to further protect consumers' rights, including the constitutional right of

privacy. The implementation of this act shall be guided by the following principles:

#### A. Consumer Rights

1. Consumers should know who is collecting their personal information and that of their children, how it is being used, and to whom it is disclosed so that they have the information necessary to exercise meaningful control over businesses' use of their personal information and that of their children.

2. Consumers should be able to control the use of their personal information, including limiting the use of their sensitive personal information, the unauthorized use or disclosure of which creates a heightened risk of harm to the consumer, and they should have meaningful options over how it is collected, used, and disclosed.

3. Consumers should have access to their personal information and should be able to correct it, delete it, and take it with them from one business to another.

4. Consumers or their authorized agents should be able to exercise these options through easily accessible self-serve tools.

5. Consumers should be able to exercise these rights without being penalized for doing so.

6. Consumers should be able to hold businesses accountable for failing to take reasonable precautions to protect their most sensitive personal information from hackers and security breaches.

7. Consumers should benefit from businesses' use of their personal information.

8. The privacy interests of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses as compared to the relationship between consumers and businesses. In addition, this law is not intended to interfere with the right to organize and collective bargaining under the National Labor Relations Act. It is the purpose and intent of the Act to extend the exemptions in this title for employee and business to business communications until January 1, 2023.

#### B. Responsibilities of Businesses

1. Businesses should specifically and clearly inform consumers about how they collect and use personal information and how they can exercise their rights and choice.

2. Businesses should only collect consumers' personal information for specific, explicit, and legitimate disclosed purposes and should not further collect, use, or disclose consumers' personal information for reasons incompatible with those purposes.

3. Businesses should collect consumers' personal information only to the extent that it is relevant and

limited to what is necessary in relation to the purposes for which it is being collected, used, and shared.

4. Businesses should provide consumers or their authorized agents with easily accessible means to allow consumers and their children to obtain their personal information, to delete it or correct it, to opt out of its sale and sharing across business platforms, services, businesses, and devices, and to limit the use of their sensitive personal information.

5. Businesses should not penalize consumers for exercising these rights.

6. Businesses should take reasonable precautions to protect consumers' personal information from a security breach.

7. Businesses should be held accountable when they violate consumers' privacy rights, and the penalties should be higher when the violation affects children.

#### C. Implementation of the Law

1. The rights of consumers and the responsibilities of businesses should be implemented with the goal of strengthening consumer privacy while giving attention to the impact on business and innovation. Consumer privacy and the development of beneficial new products and services are not necessarily incompatible goals. Strong consumer privacy rights create incentives to innovate and develop new products that are privacy protective.

2. Businesses and consumers should be provided with clear guidance about their responsibilities and rights.

3. The law should place the consumer in a position to knowingly and freely negotiate with a business over the business' use of the consumer's personal information.

4. The law should adjust to technological changes, help consumers exercise their rights, and assist businesses with compliance with the continuing goal of strengthening consumer privacy.

5. The law should enable proconsumer new products and services and promote efficiency of implementation for business provided that the amendments do not compromise or weaken consumer privacy.

6. The law should be amended, if necessary, to improve its operation, provided that the amendments do not compromise or weaken consumer privacy, while giving attention to the impact on business and innovation.

7. Businesses should be held accountable for violating the law through vigorous administrative and civil enforcement.

8. To the extent it advances consumer privacy and business compliance, the law should be compatible with privacy laws in other jurisdictions.

SEC. 4. Section 1798.100 of the Civil Code is amended to read:



*1798.100. General Duties of Businesses that Collect Personal Information*

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

~~(b) (a) A business that controls the collection of collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the of the following:~~

~~(1) The categories of personal information to be collected and the purposes for which the categories of personal information are collected or used shall be used and whether that information is sold or shared. A business shall not collect additional categories of personal information or use personal information collected for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected without providing the consumer with notice consistent with this section.~~

~~(2) If the business collects sensitive personal information, the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section.~~

~~(3) The length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period provided that a business shall not retain a consumer's personal information or sensitive personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.~~

~~(b) A business that, acting as a third party, controls the collection of personal information about a consumer may satisfy its obligation under subdivision (a) by providing the required information prominently and conspicuously on the homepage of its internet website. In addition, if a business acting as a third party controls the collection of personal information about a consumer on its premises, including in a vehicle, then the business 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 are used, and whether that personal information is sold, in a clear and conspicuous manner at the location.~~

*(c) A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes.*

*(d) A business that collects a consumer's personal information and that sells that personal information to, or shares it with, a third party or that discloses it to a service provider or contractor for a business purpose shall enter into an agreement with the third party, service provider, or contractor, that:*

*(1) Specifies that the personal information is sold or disclosed by the business only for limited and specified purposes.*

*(2) Obligates the third party, service provider, or contractor to comply with applicable obligations under this title and obligate those persons to provide the same level of privacy protection as is required by this title.*

*(3) Grants the business rights to take reasonable and appropriate steps to help ensure that the third party, service provider, or contractor uses the personal information transferred in a manner consistent with the business' obligations under this title.*

*(4) Requires the third party, service provider, or contractor to notify the business if it makes a determination that it can no longer meet its obligations under this title.*

*(5) Grants the business the right, upon notice, including under paragraph (4), to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.*

*(e) A business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.*

*(f) Nothing in this section shall require a business to disclose trade secrets, as specified in regulations adopted pursuant to paragraph (3) of subdivision (a) of Section 1798.185.*

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

~~(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if~~

~~provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.~~

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

SEC. 5. Section 1798.105 of the Civil Code is amended to read:

*1798.105. Consumers' Right to Delete Personal Information*

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

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

(c) (1) 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 notify any service providers or contractors to delete the consumer's personal information from their records, and notify all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.~~

(2) ~~The business may maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws or for other purposes, solely to the extent permissible under this title.~~

(3) ~~A service provider or contractor shall cooperate with the business in responding to a verifiable consumer request, and at the direction of the business, shall delete, or enable the business to delete and shall notify any of its own service providers or contractors to delete personal information about the consumer collected, used, processed, or retained by the service provider or the contractor. The service provider or contractor shall notify any service providers, contractors, or third parties who may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless~~

~~this proves impossible or involves disproportionate effort. A service provider or contractor shall not be required to comply with a deletion request submitted by the consumer directly to the service provider or contractor to the extent that the service provider or contractor has collected, used, processed, or retained the consumer's personal information in its role as a service provider or contractor to the business.~~

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

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

(2) ~~Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity. Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.~~

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

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

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

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of ability to complete 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 and compatible with the context in which the consumer provided the information.

(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.~~

SEC. 6. Section 1798.106 is added to the Civil Code, to read:

*1798.106. Consumers' Right to Correct Inaccurate Personal Information*

*(a) A consumer shall have the right to request a business that maintains inaccurate personal information about the consumer to correct that inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information.*

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

*(c) A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer, pursuant to Section 1798.130 and regulations adopted pursuant to paragraph (8) of subdivision (a) of Section 1798.185.*

SEC. 7. Section 1798.110 of the Civil Code is amended to read:

*1798.110. Consumers' Right to Know What Personal Information is Being Collected. Right to Access Personal Information*

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

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

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

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

(4) The categories of third parties ~~with~~ to whom the business ~~shares~~ discloses 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 *subparagraph (B) of paragraph (3) of subdivision (a) of Section 1798.130*, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer, *provided that a business shall be deemed to be in compliance with paragraphs (1) to (4), inclusive, of subdivision (a) to the extent that the categories of information and the business or commercial purpose for collecting, selling, or sharing personal information it would be required to disclose to the consumer pursuant to paragraphs (1)*

*to (4), inclusive, of subdivision (a) is the same as the information it has disclosed pursuant to paragraphs (1) to (4), inclusive, of subdivision (c).*

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

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

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

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

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

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

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

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

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

SEC. 8. Section 1798.115 of the Civil Code is amended to read:

*1798.115. Consumers' Right to Know What Personal Information is Sold or Shared and to Whom*

~~1798.115.~~ (a) A consumer shall have the right to request that a business that sells or shares 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 or shared about the consumer and the categories of third parties to whom the personal information was sold or shared, by category or categories of personal information for each category of third parties to whom the personal information was sold or shared.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose and the categories of persons to whom it was disclosed for a business purpose.

(b) A business that sells or shares 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 *or shares* 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 shared*, or if the business has not sold *or shared* 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 *or share* personal information about a consumer that has been sold to, *or shared with*, 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.

SEC. 9. Section 1798.120 of the Civil Code is amended to read:

*1798.120. Consumers' Right to Opt Out of Sale or Sharing of Personal Information*

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

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

(c) Notwithstanding subdivision (a), a business shall not sell *or share* the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale *or sharing* 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 *or share* the consumer's personal information or, in the case of a minor consumer's

personal information has not received consent to sell *or share* the minor consumer's personal information, shall be prohibited, pursuant to paragraph (4) of subdivision ~~(a)~~ (c) of Section 1798.135, from selling *or sharing* the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides ~~express authorization~~ *consent*, for the sale *or sharing* of the consumer's personal information.

SEC. 10. Section 1798.121 is added to the Civil Code, to read:

*1798.121. Consumers' Right to Limit Use and Disclosure of Sensitive Personal Information*

~~1798.121.~~ (a) A consumer shall have the right, at any time, to direct a business that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services *or provide the goods reasonably expected by an average consumer who requests those goods or services*, to perform the services set forth in paragraphs (2), (4), (5), and (8) of subdivision (e) of Section 1798.140, and as authorized by regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185. A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in this subdivision shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be used, *or disclosed to a service provider or contractor, for additional, specified purposes and that consumers have the right to limit the use or disclosure of their sensitive personal information.*

(b) A business that has received direction from a consumer not to use or disclose the consumer's sensitive personal information, except as authorized by subdivision (a), shall be prohibited, pursuant to paragraph (4) of subdivision (c) of Section 1798.135, from using or disclosing the consumer's sensitive personal information for any other purpose after its receipt of the consumer's direction unless the consumer subsequently provides consent for the use *or disclosure of the consumer's sensitive personal information for additional purposes.*

(c) A service provider or contractor that assists a business in performing the purposes authorized by subdivision (a) may not use the sensitive personal information after it has received instructions from the business and to the extent it has actual knowledge that the personal information is sensitive personal information for any other purpose. A service provider or contractor is only required to limit its use of sensitive personal information received pursuant to a written contract with the business in response to instructions from the business and only with respect to its relationship with that business.

*(d) Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this act, including Section 1798.100.*

SEC. 11. Section 1798.125 of the Civil Code is amended to read:

*1798.125. Consumers' Right of No Retaliation Following Opt Out or Exercise of Other Rights*

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

(A) Denying goods or services to the consumer.

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

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

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

*(E) Retaliating against an employee, applicant for employment, or independent contractor, as defined in subparagraph (A) of paragraph (2) of subdivision (m) of Section 1798.145, for exercising their rights under this title.*

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

*(3) This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title.*

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the deletion or retention 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 reasonably related to the value provided to the business by the consumer's data.

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

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the

business prior opt-in consent pursuant to Section 1798.130 that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time. *If a consumer refuses to provide opt-in consent, then the business shall wait for at least 12 months before next requesting that the consumer provide opt-in consent, or as prescribed by regulations adopted pursuant to Section 1798.185.*

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

SEC. 12. Section 1798.130 of the Civil Code is amended to read:

*1798.130. Notice, Disclosure, Correction, and Deletion Requirements*

~~1798.130~~ (a) In order to comply with Sections 1798.100, 1798.105, ~~1798.106~~, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, *or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively*, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, *or for requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.*

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, *or requests for deletion or correction pursuant to Sections 1798.105 and 1798.106, respectively.*

(2) (A) Disclose and deliver the required information to a consumer free of charge, *correct inaccurate personal information, or delete a consumer's personal information, based on the consumer's request*, 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, *to correct inaccurate personal information, or to delete personal information* within 45 days of receipt of the consumer's request. The time period to provide the required information, *to correct inaccurate personal information, or to delete personal 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 of the required information 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 may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request *provided that if the consumer, maintains has an account with the business, the business may require the consumer to submit the request through that account. use that account to submit a verifiable consumer request.*

*(B) The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the verifiable consumer request provided that, upon the adoption of a regulation pursuant to paragraph (9) of subdivision (a) of Section 1798.185, a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business's obligation to provide that information, shall only apply to personal information collected on or after January 1, 2022. Nothing in this subparagraph shall require a business to keep personal information for any length of time.*

*(3) (A) A business that receives a verifiable consumer request pursuant to Section 1798.110 or 1798.115 shall disclose any personal information it has collected about a consumer, directly or indirectly, including through or by a service provider or contractor, to the consumer. A service provider or contractor shall not be required to comply with a verifiable consumer request received directly from a consumer or a consumer's authorized agent, pursuant to Section 1798.110 or 1798.115, to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor. A service provider or contractor shall provide assistance to a business with which it has a contractual relationship with respect to the business' response to a verifiable consumer request, including, but not limited to, by providing to the business the consumer's personal information in the service provider or contractor's possession, which the service provider or contractor obtained as a result of providing services to the business, and by correcting inaccurate*

*information or by enabling the business to do the same. A service provider or contractor that collects personal information pursuant to a written contract with a business shall be required to assist the business through appropriate technical and organizational measures in complying with the requirements of subdivisions (d) to (f), inclusive, of Section 1798.100, taking into account the nature of the processing.*

*(B) For purposes of subdivision (b) of Section 1798.110:*

*(A) (i) 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) (ii) Identify by category or categories the personal information collected about the consumer in the preceding 12 months for the applicable period of time by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected; the categories of sources from which the consumer's personal information was collected; the business or commercial purpose for collecting, selling, or sharing the consumer's personal information; and the categories of third parties to whom the business discloses the consumer's personal information.*

*(iii) Provide the specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format that may also be transmitted to another entity at the consumer's request without hindrance. "Specific pieces of information" do not include data generated to help ensure security and integrity or as prescribed by regulation. Personal information is not considered to have been disclosed by a business when a consumer instructs a business to transfer the consumer's personal information from one business to another in the context of switching services.*

*(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 or shared in the preceding 12 months during the applicable period of time 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 or shared in*

~~the preceding 12 months during the applicable period of time~~ by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold or shared. 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 during the applicable period of time~~ 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~~ persons to whom the consumer's personal information was disclosed for a business purpose ~~in the preceding 12 months during the applicable period of time~~ by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

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

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, and 1798.125 and ~~one~~ two or more designated methods for submitting requests, *except as provided in subparagraph (A) of paragraph (1) of subdivision (a).*

(B) For purposes of subdivision (c) of Section 1798.110;:

(i) ~~a~~ 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.

(ii) *The categories of sources from which consumers' personal information is collected.*

(iii) *The business or commercial purpose for collecting, selling, or sharing consumers' personal information.*

(iv) *The categories of third parties to whom the business discloses consumers' personal information.*

(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 or shared 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 shared, or if the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall *prominently* disclose that fact *in its privacy policy.*

(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~~ describes the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.106, 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' verification of the consumer's request solely for the purposes of verification *and shall not further disclose the personal information, retain it longer than necessary for purposes of verification, or use it for unrelated purposes.*

(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 1798.100, 1798.110, and 1798.115 shall follow the ~~definition~~ definitions of personal information *and sensitive personal information* in Section 1798.140 by describing the categories of personal information using the specific terms set forth in subparagraphs (A) to (K), inclusive, of paragraph (1) of subdivision (v) of Section 1798.140 and by describing the categories of sensitive personal information using the specific terms set forth in paragraphs (1) to (9), inclusive, of subdivision (ae) of Section 1798.140.

SEC. 13. Section 1798.135 of the Civil Code is amended to read:

1798.135. *Methods of Limiting Sale, Sharing, and Use of Personal Information and Use of Sensitive Personal Information*

~~1798.135~~ (a) A business that ~~is required to comply with Section 1798.120~~ sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than those authorized by subdivision (a) of Section



1798.121 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's ~~internet internet homepage-homepages~~, titled "Do Not Sell or Share My Personal Information," to an ~~internet Web page-internet web page~~ that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or sharing of the consumer's personal information.

(2) Provide a clear and conspicuous link on the business' internet homepages, titled "Limit the Use of My Sensitive Personal Information," that enables a consumer, or a person authorized by the consumer, to limit the use or disclosure of the consumer's sensitive personal information to those uses authorized by subdivision (a) of Section 1798.121.

(3) At the business' discretion, utilize a single, clearly labeled link on the business' internet homepages, in lieu of complying with paragraphs (1) and (2), if that link easily allows a consumer to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

(4) In the event that a business responds to opt-out requests received pursuant to paragraph (1), (2), or (3) by informing the consumer of a charge for the use of any product or service, present the terms of any financial incentive offered pursuant to subdivision (b) of Section 1798.125 for the retention, use, sale, or sharing of the consumer's personal information.

(b) (1) A business shall not be required to comply with subdivision (a) if the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent by a platform, technology, or mechanism, based on technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185, to the business indicating the consumer's intent to opt out of the business' sale or sharing of the consumer's personal information or to limit the use or disclosure of the consumer's sensitive personal information, or both.

(2) A business that allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information pursuant to paragraph (1) may provide a link to a web page that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to that business' sale or sharing of the consumer's personal information or the use of the consumer's sensitive personal information for additional purposes provided that:

(A) The consent web page also allows the consumer or a person authorized by the consumer to revoke the consent as easily as it is affirmatively provided.

(B) The link to the web page does not degrade the consumer's experience on the web page the consumer intends to visit and has a similar look, feel, and size relative to other links on the same web page.

(C) The consent web page complies with technical specifications set forth in regulations adopted pursuant to paragraph (20) of subdivision (a) of Section 1798.185.

(3) A business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b).

(c) A business that is subject to this section shall:

(1) ~~not~~ Not require a consumer to create an account or provide additional information beyond what is necessary in order to direct the business not to sell or share the consumer's personal information or to limit use or disclosure of the consumer's sensitive personal information.

(2) Include a description of a consumer's rights pursuant to ~~Section~~ Sections 1798.120 and 1798.121, along with a separate link to the "Do Not Sell or Share My Personal Information" ~~internet Web page internet web page~~ and a separate link to the "Limit the Use of My Sensitive Personal Information" internet web page, if applicable, or a single link to both choices, or a statement that the business responds to and abides by opt-out preference signals sent by a platform, technology, or mechanism in accordance with subdivision (b), 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 Sections 1798.120, 1798.121, 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 or sharing of their personal information or limit the use or disclosure of their sensitive personal information, refrain from selling or sharing the consumer's personal information or using or disclosing the consumer's sensitive personal information collected by the business about the consumer and wait for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information or the use and disclosure of the consumer's sensitive personal information for additional purposes, or as authorized by regulations.

(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 consumers under 16 years of age who do not consent to the sale or sharing of their personal information, refrain from selling or sharing the personal information of the consumer under 16 years of age and wait for at least 12 months before requesting the consumer's consent again, or as authorized by regulations or until the consumer attains 16 years of age.~~

(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)~~ (d) 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.

~~(e)~~ (e) A consumer may authorize another person solely to opt-out of the sale or sharing of the consumer's personal information and to limit the use of the consumer's sensitive personal information on the consumer's behalf, including through an opt-out preference signal, as defined in paragraph (1) of subdivision (b), indicating the consumer's intent to opt out, 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 regardless of whether the business has elected to comply with subdivision (a) or (b). For purposes of clarity, a business that elects to comply with subdivision (a) may respond to the consumer's opt-out consistent with Section 1798.125.

(f) If a business communicates a consumer's opt-out request to any person authorized by the business to collect personal information, the person shall thereafter only use that consumer's personal information for a business purpose specified by the business, or as otherwise permitted by this title, and shall be prohibited from:

(1) Selling or sharing the personal information.

(2) Retaining, using, or disclosing that consumer's personal information.

(A) For any purpose other than for the specific purpose of performing the services offered to the business.

(B) Outside of the direct business relationship between the person and the business.

(C) For a commercial purpose other than providing the services to the business.

(g) A business that communicates a consumer's opt-out request to a person pursuant to subdivision (f) shall not be liable under this title if the person receiving the opt-out request violates the restrictions set forth in the title provided that, at the time of communicating the opt-out request, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation. Any provision of a contract or agreement of any kind that purports to waive or limit in any way this subdivision shall be void and unenforceable.

SEC. 14. Section 1798.140 of the Civil Code is amended to read:

1798.140. Definitions

~~1798.140.~~ For purposes of this title:

(a) "Advertising and marketing" means a communication by a business or a person acting on the business' behalf in any medium intended to induce a consumer to obtain goods, services, or employment.

~~(a)~~ (b) "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)~~ (c) "Biometric information" means an individual's physiological, biological or behavioral characteristics, including information pertaining to an individual's deoxyribonucleic acid (DNA), that can be used or is intended to 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.

~~(e)~~ (d) "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~~ *As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars (\$25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.*

(B) ~~Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 100,000 or more consumers or; households, or devices.~~

(C) ~~Derives 50 percent or more of its annual revenues from selling or sharing 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 *and with whom the business shares consumers' personal information.* "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 *that the average consumer would understand that two or more entities are commonly owned.*

(3) *A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.*

(4) *A person that does business in California, that is not covered by paragraph (1), (2), or (3) and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.*

~~(d)~~ (e) "Business purpose" means the use of personal information for the business's ~~or a service provider's~~ operational purposes, or other notified purposes, *or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (11) of subdivision (a) of Section 1798.185, 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. Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.~~

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

(4) Short-term, transient use, *including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about a the consumer or otherwise alter an individual the consumer's experience outside the current interaction with the business., 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, *providing storage,* or providing similar services on behalf of the business ~~or service provider.~~

~~(6) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.~~

~~(6)~~ (7) Undertaking internal research for technological development and demonstration.

~~(7)~~ (8) 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)~~ (f) "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) (g)~~ "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.~~

(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent.

~~(g)~~ (i) "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.

(j) (1) "Contractor" means a person to whom the business makes available a consumer's personal information for a business purpose, pursuant to a written contract with the business, provided that the contract:

(A) Prohibits the contractor from:

(i) Selling or sharing the personal information.

(ii) Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract, or as otherwise permitted by this title.

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

(iv) Combining the personal information that the contractor receives pursuant to a written contract with the business with personal information that it receives from or on behalf of another person or persons, or collects from its own interaction with the consumer,

provided that the contractor may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) and in regulations adopted by the California Privacy Protection Agency.

(B) Includes a certification made by the contractor that the contractor understands the restrictions in subparagraph (A) and will comply with them.

(C) Permits, subject to agreement with the contractor, the business to monitor the contractor's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a contractor engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the contractor engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(k) "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts.

(l) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice, as further defined by regulation.

~~(h)~~ (m) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information:

(1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household.

(2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision.

(3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision. ~~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) (n) "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) (o) "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) (p) "Homepage" means the introductory page of an internet website 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 notices required by subdivision (a) of Section 1798.135 this title, including, but not limited to, before downloading the application.~~

~~(q) "Household" means a group, however identified, of consumers who cohabit with one another at the same residential address and share use of common devices or services.~~

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

~~(s) "Intentionally interacts" means when the consumer intends to interact with a person, or disclose personal information to a person, via one or more deliberate interactions, including visiting the person's website or purchasing a good or service from the~~

~~person. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a person.~~

~~(t) "Nonpersonalized advertising" means advertising and marketing that is based solely on a consumer's personal information derived from the consumer's current interaction with the business with the exception of the consumer's precise geolocation.~~

~~(n) (u) "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.~~

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

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

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

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

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

~~(E) Biometric information.~~

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

~~(G) Geolocation data.~~

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

~~(I) Professional or employment-related information.~~

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

~~(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions,~~

behavior, attitudes, intelligence, abilities, and aptitudes.

(L) *Sensitive personal information.*

(2) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern. For purposes of this paragraph, "publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge.

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

(w) *"Precise geolocation" means any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of 1,850 feet, except as prescribed by regulations.*

(p) (x) "Probabilistic identifier" means the identification of a consumer or a consumer's 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) (y) "Processing" means any operation or set of operations that are performed on personal data information or on sets of personal data information, whether or not by automated means.

(z) *"Profiling" means any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185, to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.*

(t) (aa) "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) (ab) "Research" means scientific analysis, systematic study and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge in the public interest and that adheres or otherwise conforms to all other applicable ethics and privacy laws, or including, but not limited to, 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, by a business.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research.

(4) Subject to business processes that specifically prohibit reidentification of the information, other than as needed to support the research.

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

(6) Protected from any reidentification attempts.

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

(8) ~~Not be used for any commercial purpose.~~

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

(ac) *"Security and integrity" means the ability of:*

(1) Networks or information systems to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information.

(2) Businesses to detect security incidents, resist malicious, deceptive, fraudulent, or illegal actions and to help prosecute those responsible for those actions.

(3) Businesses to ensure the physical safety of natural persons.

(t) (ad) (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:

(i) Disclose personal information.

~~(ii) Uses the business to intentionally interact with a one or more third party parties, 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 *or limited the use of the consumer's sensitive personal information* for the purposes of alerting ~~third parties~~ persons that the consumer has opted out of the sale of the consumer's personal information *or limited the use of the consumer's sensitive personal information*.

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

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

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

~~(D)~~ (C) 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 *this title*. 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 title*. 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).

(ae) "Sensitive personal information" means:

(1) Personal information that reveals:

(A) A consumer's social security, driver's license, state identification card, or passport number.

(B) A consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

(C) A consumer's precise geolocation.

(D) A consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership.

(E) The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication.

(F) A consumer's genetic data.

(2) (A) The processing of biometric information for the purpose of uniquely identifying a consumer.

(B) Personal information collected and analyzed concerning a consumer's health.

(C) Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

(3) Sensitive personal information that is "publicly available" pursuant to paragraph (2) of subdivision (v) shall not be considered sensitive personal information or personal information.

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

~~(v)~~ (ag) (1) "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, *person* that processes personal information on behalf of a business and ~~to which that receives from or on behalf of 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~~ *person* from:

(A) Selling or sharing the personal information.

(B) Retaining, using, or disclosing the personal information for any purpose other than for the ~~specific purpose of performing the services-business purposes 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 the business purposes specified in the contract with the business, or as otherwise permitted by this title~~.

(C) Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business.

(D) Combining the personal information that the service provider receives from, or on behalf of, the

business with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose as defined in regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, except as provided for in paragraph (6) of subdivision (e) of this section and in regulations adopted by the California Privacy Protection Agency. The contract may, subject to agreement with the service provider, permit the business to monitor the service provider's compliance with the contract through measures, including, but not limited to, ongoing manual reviews and automated scans and regular assessments, audits, or other technical and operational testing at least once every 12 months.

(2) If a service provider engages any other person to assist it in processing personal information for a business purpose on behalf of the business, or if any other person engaged by the service provider engages another person to assist in processing personal information for that business purpose, it shall notify the business of that engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth in paragraph (1).

(ah) (1) "Share," "shared," or "sharing" means sharing, 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 a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

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

(A) A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

(B) The business uses or shares an identifier for a consumer who has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sharing of the consumer's personal information or limited the use of the consumer's sensitive personal information.

(C) 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 this title. 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 this title. 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).

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

(1) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business consumers under this title.

(2) A service provider to the business.

(3) A contractor.

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

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

~~(I) Selling the personal information.~~

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

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

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

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



(\*) (aj) "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 that is linked to a consumer or family. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children under 18 years of age over which the parent or guardian has custody.

(y) (ak) "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, or by a person who has power of attorney or is acting as a conservator for the consumer, and that the business can reasonably verify, using commercially reasonable methods, 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, to delete personal information pursuant to Section 1798.105, or to correct inaccurate personal information pursuant to Section 1798.106, if the business cannot verify, pursuant to this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

SEC. 15. Section 1798.145 of the Civil Code is amended to read:

*1798.145. Exemptions*

~~1798.145.~~ (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 or comply with a court order or subpoena to provide information.
- (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities. *Law enforcement agencies, including police and sheriff's departments, may direct a business pursuant to a law enforcement agency-approved investigation with an active case number not to delete a consumer's personal information, and upon receipt of that direction, a business shall not delete the personal information for 90 days in order to allow the law enforcement agency to obtain a court-issued*

*subpoena, order, or warrant to obtain a consumer's personal information. For good cause and only to the extent necessary for investigatory purposes, a law enforcement agency may direct a business not to delete the consumer's personal information for additional 90-day periods. A business that has received direction from a law enforcement agency not to delete the personal information of a consumer who has requested deletion of the consumer's personal information shall not use the consumer's personal information for any purpose other than retaining it to produce to law enforcement in response to a court-issued subpoena, order, or warrant unless the consumer's deletion request is subject to an exemption from deletion under this title.*

(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) Cooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury provided that:

(A) The request is approved by a high-ranking agency officer for emergency access to a consumer's personal information.

(B) The request is based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis.

(C) The agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.

~~(4)~~ (5) Exercise or defend legal claims.

~~(5)~~ (6) Collect, use, retain, sell, share, or disclose ~~consumer~~ consumers' personal information that is deidentified or in the aggregate consumer information.

~~(6)~~ (7) Collect, or sell, or share 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~~ prohibit 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, 1798.115, 1798.120, 1798.121, 1798.130, and ~~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) ~~Personal information~~ information collected as part of a clinical trial *or other biomedical research study* subject to, *or conducted in accordance with*, 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, *provided that the information is not sold or shared in a manner not permitted by this subparagraph, and if it is inconsistent, that participants be informed of that use and provide consent.*

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

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general

reputation, personal characteristics, or mode of living by a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code.

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

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

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant ~~pursuant~~ subject 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), *or the federal Farm Credit Act of 1971 (as amended in 12 U.S.C. 2001-2279cc and implementing regulations, 12 C.F.R. 600, et seq.)*. This subdivision shall not apply to Section 1798.150.

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

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

(2) For purposes of this subdivision:

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

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

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

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

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

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

~~(2) For purposes of this subdivision:~~

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

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

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

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

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

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

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

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

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

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

~~(i) (h) 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 a consumer for any verified verifiable consumer request may be extended by up to a total of 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 verifiable consumer request is manifestly unfounded or excessive.~~

~~(j) (i) (1) A business that discloses personal information to a service provider or contractor in compliance with this title shall not be liable under this title if the service provider or contractor 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 or contractor intends to commit such a violation. A service provider or contractor 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 provided that the service provider or contractor shall be liable for its own violations of this title.~~

~~(2) A business that discloses personal information of a consumer, with the exception of consumers who have exercised their right to opt out of the sale or~~

sharing of their personal information, consumers who have limited the use or disclosure of their sensitive personal information, and minor consumers who have not opted in to the collection or sale of their personal information, to a third party pursuant to a written contract that requires the third party to provide the same level of protection of the consumer's rights under this title as provided by the business shall not be liable under this title if the third party 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 third party intends to commit such a violation.

~~(k)~~ (j) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or, service provider, or contractor to:

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

(2) Retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained.

(3) Maintain information in identifiable, linkable, or associable form, or collect, obtain, retain, or access any data or technology, in order to be capable of linking or associating a verifiable consumer request with personal information.

~~(A)~~ (k) 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 natural persons. A verifiable consumer request for specific pieces of personal information, pursuant to Section 1798.110 to delete a consumer's personal information, pursuant to Section 1798.105, or to correct inaccurate personal information, pursuant to Section 1798.106, shall not extend to personal information about the consumer that belongs to, or the business maintains on behalf of, another natural person. A business may rely on representations made in a verifiable consumer request as to rights with respect to personal information and is under no legal requirement to seek out other persons that may have or claim to have rights to personal information, and a business is under no legal obligation under this title or any other provision of law to take any action under this title in the event of a dispute between or among persons claiming rights to personal information in the business' possession.

~~(m)~~ (l) 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.

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

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

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

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

(2) For purposes of this subdivision:

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

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

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

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

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

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

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

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

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

(4) This subdivision shall become inoperative on January 1, 2023.

(n) (1) The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.121, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who acted or is acting as an employee, owner, director, officer, or independent contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.

(2) For purposes of this subdivision:

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

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

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

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

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

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

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

(3) This subdivision shall become inoperative on January 1, ~~2021~~, 2023.

(o) (1) Sections 1798.105 and 1798.120 shall not apply to a commercial credit reporting agency's collection, processing, sale, or disclosure of business controller information to the extent the commercial credit reporting agency uses the business controller information solely to identify the relationship of a consumer to a business that the consumer owns or contact the consumer only in the consumer's role as the owner, director, officer, or management employee of the business.

(2) For the purposes of this subdivision:

(A) "Business controller information" means the name or names of the owner or owners, director, officer, or management employee of a business and the contact information, including a business title, for the owner or owners, director, officer, or management employee.

(B) "Commercial credit reporting agency" has the meaning set forth in subdivision (b) of Section 1785.42.

(C) "Owner" means a natural person that meets one of the following:

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

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

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

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

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

(F) "Management employee" means a natural person whose name and contact information is reported to or collected by a commercial credit reporting agency as the primary manager of a business and used solely within the context of the natural person's role as the primary manager of the business.

(p) The obligations imposed on businesses in Sections 1798.105, 1798.106, 1798.110, and 1798.115 shall not apply to household data.

(q) (1) This title does not require a business to comply with a verifiable consumer request to delete a consumer's personal information under Section 1798.105 to the extent the verifiable consumer request applies to a student's grades, educational scores, or educational test results that the business

holds on behalf of a local educational agency, as defined in subdivision (d) of Section 49073.1 of the Education Code, at which the student is currently enrolled. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(2) This title does not require, in response to a request pursuant to Section 1798.110, that a business disclose on educational standardized assessment or educational assessment or a consumer's specific responses to the educational standardized assessment or educational assessment if consumer access, possession, or control would jeopardize the validity and reliability of that educational standardized assessment or educational assessment. If a business does not comply with a request pursuant to this section, it shall notify the consumer that it is acting pursuant to this exception.

(3) For purposes of this subdivision:

(A) "Educational standardized assessment or educational assessment" means a standardized or nonstandardized quiz, test, or other assessment used to evaluate students in or for entry to kindergarten and grades 1 to 12, inclusive, schools, postsecondary institutions, vocational programs, and postgraduate programs that are accredited by an accrediting agency or organization recognized by the State of California or the United States Department of Education, as well as certification and licensure examinations used to determine competency and eligibility to receive certification or licensure from a government agency or government certification body.

(B) "Jeopardize the validity and reliability of that educational standardized assessment or educational assessment" means releasing information that would provide an advantage to the consumer who has submitted a verifiable consumer request or to another natural person.

(r) Sections 1798.105 and 1798.120 shall not apply to a business' use, disclosure, or sale of particular pieces of a consumer's personal information if the consumer has consented to the business' use, disclosure, or sale of that information to produce a physical item, including a school yearbook containing the consumer's photograph if:

(1) The business has incurred significant expense in reliance on the consumer's consent.

(2) Compliance with the consumer's request to opt out of the sale of the consumer's personal information or to delete the consumer's personal information would not be commercially reasonable.

(3) The business complies with the consumer's request as soon as it is commercially reasonable to do so.

SEC. 16. Section 1798.150 of the Civil Code is amended to read:

1798.150. *Personal Information Security Breaches*

~~1798.150.~~ (a) (1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, or whose email address in combination with a password or security question and answer that would permit access to the account 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. *The implementation and maintenance of reasonable security procedures and practices pursuant to Section 1798.81.5 following a breach does not constitute a cure with respect to that breach.* 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.

SEC. 17. Section 1798.155 of the Civil Code is amended to read:

*1798.155. Administrative Enforcement*

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

~~(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, contractor, or other person that violates this title shall be subject to an injunction and liable for an administrative fine 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 or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge are under 16 years of age, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, in an administrative enforcement action brought by the California Privacy Protection Agency. 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) (b) Any civil penalty administrative fine assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b) (a), 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, and the California Privacy Protection Agency in connection with this title.~~

SEC. 18. Section 1798.160 of the Civil Code is amended to read:

*1798.160. Consumer Privacy Fund*

~~1798.160. (a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature first to offset any costs incurred by the state courts in connection with actions brought to enforce this title, and any the costs incurred by the Attorney General in carrying out the Attorney General's duties under this title, and then for the purposes of establishing an investment fund in the State Treasury, with any earnings or interest from the fund to be deposited in the General Fund, and making grants to promote and protect consumer privacy, educate children in the area of online privacy, and fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.~~

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively as follows:

(1) ~~To offset any costs incurred by the state courts and the Attorney General in connection with this title.~~

(2) *After satisfying the obligations under paragraph (1), the remaining funds shall be allocated each fiscal year as follows:*

(A) *Ninety-one percent shall be invested by the Treasurer in financial assets with the goal of maximizing long term yields consistent with a prudent level of risk. The principal shall not be subject to transfer or appropriation, provided that any interest and earnings shall be transferred on an annual basis to the General Fund for appropriation by the Legislature for General Fund purposes.*

(B) *Nine percent shall be made available to the California Privacy Protection Agency for the purposes of making grants in California, with 3 percent allocated to each of the following grant recipients:*

(i) *Nonprofit organizations to promote and protect consumer privacy.*

(ii) *Nonprofit organizations and public agencies, including school districts, to educate children in the area of online privacy.*

(iii) *State and local law enforcement agencies to fund cooperative programs with international law enforcement organizations to combat fraudulent activities with respect to consumer data breaches.*

~~(c) These funds Funds in the Consumer Privacy Fund 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.~~

SEC. 19. Section 1798.175 of the Civil Code is amended to read:

*1798.175. Conflicting Provisions*

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

SEC. 20. Section 1798.180 of the Civil Code is amended to read:

*1798.180. Preemption*

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

SEC. 21. Section 1798.185 of the Civil Code is amended to read:

*1798.185. Regulations*

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

(1) Updating ~~or adding as needed~~ additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision ~~(e)~~ (v) of Section 1798.140, and updating or adding categories of sensitive personal information to those enumerated in subdivision (ae) 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~~ definitions of "deidentified" and ~~unique~~ identifiers "unique identifier" to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and ~~additional~~ adding, modifying, or deleting 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. *The authority to update the definition of "deidentified" shall not apply to deidentification standards set forth in Section 164.514 of Title 45 of the Code of Federal*

*Regulations, where such information previously was "protected health information" as defined in Section 160.103 of Title 45 of the Code of Federal Regulations.*

(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, *with the intention that trade secrets should not be disclosed in response to a verifiable consumer request.*

(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 or sharing of personal information pursuant to Section 1798.120 and to limit the use of a consumer's sensitive personal information pursuant to Section 1798.121 to ensure that consumers have the ability to exercise their choices without undue burden and to prevent business from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision to opt out of the sale or sharing of their personal information or to limit the use of their sensitive personal information.

(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~~ thresholds, in January of every odd-numbered year to reflect any increase in the Consumer Price Index, in: subparagraph (A) of paragraph (1) of subdivision (e) (d) of Section 1798.140; subparagraph (A) of paragraph (1) of subdivision (a) of Section 1798.150; subdivision (a) of Section 1798.155; Section 1798.199.25; and subdivision (a) of Section 1798.199.90 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 incentives ~~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 1798.105, 1798.106, 1798.110, and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's



ability to delete personal information, correct inaccurate personal information pursuant to Section 1798.106, or obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received from a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(8) Establishing how often, and under what circumstances, a consumer may request a correction pursuant to Section 1798.106, including standards governing the following:

(A) How a business responds to a request for correction, including exceptions for requests to which a response is impossible or would involve disproportionate effort, and requests for correction of accurate information.

(B) How concerns regarding the accuracy of the information may be resolved.

(C) The steps a business may take to prevent fraud.

(D) If a business rejects a request to correct personal information collected and analyzed concerning a consumer's health, the right of a consumer to provide a written addendum to the business with respect to any item or statement regarding any such personal information that the consumer believes to be incomplete or incorrect. The addendum shall be limited to 250 words per alleged incomplete or incorrect item and shall clearly indicate in writing that the consumer requests the addendum to be made a part of the consumer's record.

(9) Establishing the standard to govern a business' determination, pursuant to subparagraph (B) of paragraph (2) of subdivision (a) of Section 1798.130, that providing information beyond the 12-month period in a response to a verifiable consumer request is impossible or would involve a disproportionate effort.

(10) Issuing regulations further defining and adding to the business purposes, including other notified purposes, for which businesses, service providers, and contractors may use consumers' personal information consistent with consumers' expectations, and further defining the business purposes for which service providers and contractors may combine consumers' personal information obtained from different sources,

except as provided for in paragraph (6) of subdivision (e) of Section 1798.140.

(11) Issuing regulations identifying those business purposes, including other notified purposes, for which service providers and contractors may use consumers' personal information received pursuant to a written contract with a business, for the service provider or contractor's own business purposes, with the goal of maximizing consumer privacy.

(12) Issuing regulations to further define "intentionally interacts," with the goal of maximizing consumer privacy.

(13) Issuing regulations to further define "precise geolocation," including if the size defined is not sufficient to protect consumer privacy in sparsely populated areas or when the personal information is used for normal operational purposes, including billing.

(14) Issuing regulations to define the term "specific pieces of information obtained from the consumer" with the goal of maximizing a consumer's right to access relevant personal information while minimizing the delivery of information to a consumer that would not be useful to the consumer, including system log information and other technical data. For delivery of the most sensitive personal information, the regulations may require a higher standard of authentication provided that the agency shall monitor the impact of the higher standard on the right of consumers to obtain their personal information to ensure that the requirements of verification do not result in the unreasonable denial of verifiable consumer requests.

(15) Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(A) Perform a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent. The factors to be considered in determining when processing may result in significant risk to the security of personal information shall include the size and complexity of the business and the nature and scope of processing activities.

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits



resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

(16) Issuing regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

(17) Issuing regulations to further define a "law enforcement agency-approved investigation" for purposes of the exception in paragraph (2) of subdivision (a) of Section 1798.145.

(18) Issuing regulations to define the scope and process for the exercise of the agency's audit authority, to establish criteria for selection of persons to audit, and to protect consumers' personal information from disclosure to an auditor in the absence of a court order, warrant, or subpoena.

(19) (A) Issuing regulations to define the requirements and technical specifications for an opt-out preference signal sent by a platform, technology, or mechanism, to indicate a consumer's intent to opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information. The requirements and specifications for the opt-out preference signal should be updated from time to time to reflect the means by which consumers interact with businesses, and should:

(i) Ensure that the manufacturer of a platform or browser or device that sends the opt-out preference signal cannot unfairly disadvantage another business.

(ii) Ensure that the opt-out preference signal is consumer-friendly, clearly described, and easy to use by an average consumer and does not require that the consumer provide additional information beyond what is necessary.

(iii) Clearly represent a consumer's intent and be free of defaults constraining or presupposing that intent.

(iv) Ensure that the opt-out preference signal does not conflict with other commonly used privacy settings or tools that consumers may employ.

(v) Provide a mechanism for the consumer to selectively consent to a business' sale of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, without affecting the consumer's preferences with respect to other businesses or disabling the opt-out preference signal globally.

(vi) State that in the case of a page or setting view that the consumer accesses to set the opt-out

preference signal, the consumer should see up to three choices, including:

(I) Global opt out from sale and sharing of personal information, including a direction to limit the use of sensitive personal information.

(II) Choice to "Limit the Use of My Sensitive Personal Information."

(III) Choice titled "Do Not Sell/Do Not Share My Personal Information for Cross-Context Behavioral Advertising."

(B) Issuing regulations to establish technical specifications for an opt-out preference signal that allows the consumer, or the consumer's parent or guardian, to specify that the consumer is less than 13 years of age or at least 13 years of age and less than 16 years of age.

(C) Issuing regulations, with the goal of strengthening consumer privacy while considering the legitimate operational interests of businesses, to govern the use or disclosure of a consumer's sensitive personal information, notwithstanding the consumer's direction to limit the use or disclosure of the consumer's sensitive personal information, including:

(i) Determining any additional purposes for which a business may use or disclose a consumer's sensitive personal information.

(ii) Determining the scope of activities permitted under paragraph (8) of subdivision (e) of Section 1798.140, as authorized by subdivision (a) of Section 1798.121, to ensure that the activities do not involve health-related research.

(iii) Ensuring the functionality of the business' operations.

(iv) Ensuring that the exemption in subdivision (d) of Section 1798.121 for sensitive personal information applies to information that is collected or processed incidentally, or without the purpose of inferring characteristics about a consumer, while ensuring that businesses do not use the exemption for the purpose of evading consumers' rights to limit the use and disclosure of their sensitive personal information under Section 1798.121.

(20) Issuing regulations to govern how a business that has elected to comply with subdivision (b) of Section 1798.135 responds to the opt-out preference signal and provides consumers with the opportunity subsequently to consent to the sale or sharing of their personal information or the use and disclosure of their sensitive personal information for purposes in addition to those authorized by subdivision (a) of Section 1798.121. The regulations should:

(A) Strive to promote competition and consumer choice and be technology neutral.

(B) Ensure that the business does not respond to an opt-out preference signal by:

(i) Intentionally degrading the functionality of the consumer experience.

(ii) Charging the consumer a fee in response to the consumer's opt-out preferences.

(iii) Making any products or services not function properly or fully for the consumer, as compared to consumers who do not use the opt-out preference signal.

(iv) Attempting to coerce the consumer to opt in to the sale or sharing of the consumer's personal information, or the use or disclosure of the consumer's sensitive personal information, by stating or implying that the use of the opt-out preference signal will adversely affect the consumer as compared to consumers who do not use the opt-out preference signal, including stating or implying that the consumer will not be able to use the business' products or services or that those products or services may not function properly or fully.

(v) Displaying any notification or pop-up in response to the consumer's opt-out preference signal.

(C) Ensure that any link to a web page or its supporting content that allows the consumer to consent to opt in:

(i) Is not part of a popup, notice, banner, or other intrusive design that obscures any part of the web page the consumer intended to visit from full view or that interferes with or impedes in any way the consumer's experience visiting or browsing the web page or website the consumer intended to visit.

(ii) Does not require or imply that the consumer must click the link to receive full functionality of any products or services, including the website.

(iii) Does not make use of any dark patterns.

(iv) Applies only to the business with which the consumer intends to interact.

(D) Strive to curb coercive or deceptive practices in response to an opt-out preference signal but should not unduly restrict businesses that are trying in good faith to comply with Section 1798.135.

(21) Review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of this title. Upon completing its review, the agency shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

(22) Harmonizing the regulations governing opt-out mechanisms, notices to consumers, and other operational mechanisms in this title to promote clarity and the functionality of this title for consumers.

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

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

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

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

(d) *Notwithstanding subdivision (a), the timeline for adopting final regulations required by the act adding this subdivision shall be July 1, 2022. Beginning the later of July 1, 2021, or six months after the agency provides notice to the Attorney General that it is prepared to begin rulemaking under this title, the authority assigned to the Attorney General to adopt regulations under this section shall be exercised by the California Privacy Protection Agency. Notwithstanding any other law, civil and administrative enforcement of the provisions of law added or amended by this act shall not commence until July 1, 2023, and shall only apply to violations occurring on or after that date. Enforcement of provisions of law contained in the California Consumer Privacy Act of 2018 amended by this act shall remain in effect and shall be enforceable until the same provisions of this act become enforceable.*

SEC. 22. Section 1798.190 of the Civil Code is amended to read:

1798.190. *Anti-Avoidance*

~~1798.190.~~ *A court or the agency shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title:*

(a) 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; or share.

(b) *If steps or transactions were taken to purposely avoid the definition of sell or share by eliminating any monetary or other valuable consideration, including by entering into contracts that do not include an exchange for monetary or other valuable consideration, but where a party is obtaining something of value or use a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.*

SEC. 23. Section 1798.192 of the Civil Code is amended to read:

1798.192. *Waiver*

~~1798.192.~~ Any provision of a contract or agreement of any kind, *including a representative action waiver*, 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~~ opt out of a business's sale of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out.

SEC. 24. *Establishment of California Privacy Protection Agency.*

SEC. 24.1. Section 1798.199.10 is added to the Civil Code, to read:

*1798.199.10. (a) There is hereby established in state government the California Privacy Protection Agency, which is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018. The agency shall be governed by a five-member board, including the chairperson. The chairperson and one member of the board shall be appointed by the Governor. The Attorney General, Senate Rules Committee, and Speaker of the Assembly shall each appoint one member. These appointments should be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.*

*(b) The initial appointments to the agency shall be made within 90 days of the effective date of the act adding this section.*

SEC. 24.2. Section 1798.199.15 is added to the Civil Code, to read:

*1798.199.15. Members of the agency board shall:*

*(a) Have qualifications, experience, and skills, in particular in the areas of privacy and technology, required to perform the duties of the agency and exercise its powers.*

*(b) Maintain the confidentiality of information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, except to the extent that disclosure is required by the Public Records Act.*

*(c) Remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from another.*

*(d) Refrain from any action incompatible with their duties and engaging in any incompatible occupation, whether gainful or not, during their term.*

*(e) Have the right of access to all information made available by the agency to the chairperson.*

*(f) Be precluded, for a period of one year after leaving office, from accepting employment with a business that was subject to an enforcement action or civil*

*action under this title during the member's tenure or during the five-year period preceding the member's appointment.*

*(g) Be precluded for a period of two years after leaving office from acting, for compensation, as an agent or attorney for, or otherwise representing, any other person in a matter pending before the agency if the purpose is to influence an action of the agency.*

SEC. 24.3. Section 1798.199.20 is added to the Civil Code, to read:

*1798.199.20. Members of the agency board, including the chairperson, shall serve at the pleasure of their appointing authority but shall serve for no longer than eight consecutive years.*

SEC. 24.4. Section 1798.199.25 is added to the Civil Code, to read:

*1798.199.25. For each day on which they engage in official duties, members of the agency board shall be compensated at the rate of one hundred dollars (\$100), adjusted biennially to reflect changes in the cost of living, and shall be reimbursed for expenses incurred in performance of their official duties.*

SEC. 24.5. Section 1798.199.30 is added to the Civil Code, to read:

*1798.199.30. The agency board shall appoint an executive director who shall act in accordance with agency policies and regulations and with applicable law. The agency shall appoint and discharge officers, counsel, and employees, consistent with applicable civil service laws, and shall fix the compensation of employees and prescribe their duties. The agency may contract for services that cannot be provided by its employees.*

SEC. 24.6. Section 1798.199.35 is added to the Civil Code, to read:

*1798.199.35. The agency board may delegate authority to the chairperson or the executive director to act in the name of the agency between meetings of the agency, except with respect to resolution of enforcement actions and rulemaking authority.*

SEC. 24.7. Section 1798.199.40 is added to the Civil Code, to read:

*1798.199.40. The agency shall perform the following functions:*

*(a) Administer, implement, and enforce through administrative actions this title.*

*(b) On and after the earlier of July 1, 2021, or within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities under this title, adopt, amend, and rescind regulations pursuant to Section 1798.185 to carry out the purposes and provisions of the California Consumer Privacy Act of 2018, including regulations specifying record keeping*

requirements for businesses to ensure compliance with this title.

(c) Through the implementation of this title, protect the fundamental privacy rights of natural persons with respect to the use of their personal information.

(d) Promote public awareness and understanding of the risks, rules, responsibilities, safeguards, and rights in relation to the collection, use, sale, and disclosure of personal information, including the rights of minors with respect to their own information, and provide a public report summarizing the risk assessments filed with the agency pursuant to paragraph (15) of subdivision (a) of Section 1798.185 while ensuring that data security is not compromised.

(e) Provide guidance to consumers regarding their rights under this title.

(f) Provide guidance to businesses regarding their duties and responsibilities under this title and appoint a Chief Privacy Auditor to conduct audits of businesses to ensure compliance with this title pursuant to regulations adopted pursuant to paragraph (18) of subdivision (a) of Section 1798.185.

(g) Provide technical assistance and advice to the Legislature, upon request, with respect to privacy-related legislation.

(h) Monitor relevant developments relating to the protection of personal information and in particular, the development of information and communication technologies and commercial practices.

(i) Cooperate with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections.

(j) Establish a mechanism pursuant to which persons doing business in California that do not meet the definition of business set forth in paragraph (1), (2), or (3) of subdivision (d) of Section 1798.140 may voluntarily certify that they are in compliance with this title, as set forth in paragraph (4) of subdivision (d) of Section 1798.140, and make a list of those entities available to the public.

(k) Solicit, review, and approve applications for grants to the extent funds are available pursuant to paragraph (2) of subdivision (b) of Section 1798.160.

(l) Perform all other acts necessary or appropriate in the exercise of its power, authority, and jurisdiction and seek to balance the goals of strengthening consumer privacy while giving attention to the impact on businesses.

SEC. 24.8. Section 1798.199.45 is added to the Civil Code, to read:

1798.199.45. (a) Upon the sworn complaint of any person or on its own initiative, the agency may investigate possible violations of this title relating to any business, service provider, contractor, or person.

The agency may decide not to investigate a complaint or decide to provide a business with a time period to cure the alleged violation. In making a decision not to investigate or provide more time to cure, the agency may consider the following:

(1) Lack of intent to violate this title.

(2) Voluntary efforts undertaken by the business, service provider, contractor, or person to cure the alleged violation prior to being notified by the agency of the complaint.

(b) The agency shall notify in writing the person who made the complaint of the action, if any, the agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction.

SEC. 24.9. Section 1798.199.50 is added to the Civil Code, to read:

1798.199.50. No finding of probable cause to believe this title has been violated shall be made by the agency unless, at least 30 days prior to the agency's consideration of the alleged violation, the business, service provider, contractor, or person alleged to have violated this title is notified of the violation by service of process or registered mail with return receipt requested, provided with a summary of the evidence, and informed of their right to be present in person and represented by counsel at any proceeding of the agency held for the purpose of considering whether probable cause exists for believing the person violated this title. Notice to the alleged violator shall be deemed made on the date of service, the date the registered mail receipt is signed, or if the registered mail receipt is not signed, the date returned by the post office. A proceeding held for the purpose of considering probable cause shall be private unless the alleged violator files with the agency a written request that the proceeding be public.

SEC. 24.10. Section 1798.199.55 is added to the Civil Code, to read:

1798.199.55. (a) When the agency determines there is probable cause for believing this title has been violated, it shall hold a hearing to determine if a violation has or violations have occurred. Notice shall be given and the hearing conducted in accordance with the Administrative Procedure Act (Chapter 5 (commencing with Section 11500), Part 1, Division 3, Title 2, Government Code). The agency shall have all the powers granted by that chapter. If the agency determines on the basis of the hearing conducted pursuant to this subdivision that a violation or violations have occurred, it shall issue an order that may require the violator to do all or any of the following:

(1) Cease and desist violation of this title.

(2) Subject to Section 1798.155, pay an administrative fine of up to two thousand five hundred dollars (\$2,500) for each violation, or up to seven

thousand five hundred dollars (\$7,500) for each intentional violation and each violation involving the personal information of minor consumers to the Consumer Privacy Fund within the General Fund of the state. When the agency determines that no violation has occurred, it shall publish a declaration so stating.

(b) If two or more persons are responsible for any violation or violations, they shall be jointly and severally liable.

SEC. 24.11. Section 1798.199.60 is added to the Civil Code, to read:

1798.199.60. Whenever the agency rejects the decision of an administrative law judge made pursuant to Section 11517 of the Government Code, the agency shall state the reasons in writing for rejecting the decision.

SEC. 24.12. Section 1798.199.65 is added to the Civil Code, to read:

1798.199.65. The agency may subpoena witnesses, compel their attendance and testimony, administer oaths and affirmations, take evidence and require by subpoena the production of any books, papers, records, or other items material to the performance of the agency's duties or exercise of its powers, including, but not limited to, its power to audit a business' compliance with this title.

SEC. 24.13. Section 1798.199.70 is added to the Civil Code, to read:

1798.199.70. No administrative action brought pursuant to this title alleging a violation of any of the provisions of this title shall be commenced more than five years after the date on which the violation occurred.

(a) The service of the probable cause hearing notice, as required by Section 1798.199.50, upon the person alleged to have violated this title shall constitute the commencement of the administrative action.

(b) If the person alleged to have violated this title engages in the fraudulent concealment of the person's acts or identity, the five-year period shall be tolled for the period of the concealment. For purposes of this subdivision, "fraudulent concealment" means the person knows of material facts related to the person's duties under this title and knowingly conceals them in performing or omitting to perform those duties for the purpose of defrauding the public of information to which it is entitled under this title.

(c) If, upon being ordered by a superior court to produce any documents sought by a subpoena in any administrative proceeding under this title, the person alleged to have violated this title fails to produce documents in response to the order by the date ordered to comply therewith, the five-year period shall be tolled for the period of the delay from the date of

filing of the motion to compel until the date the documents are produced.

SEC. 24.14. Section 1798.199.75 is added to the Civil Code, to read:

1798.199.75. (a) In addition to any other available remedies, the agency may bring a civil action and obtain a judgment in superior court for the purpose of collecting any unpaid administrative fines imposed pursuant to this title after exhaustion of judicial review of the agency's action. The action may be filed as a small claims, limited civil, or unlimited civil case depending on the jurisdictional amount. The venue for this action shall be in the county where the administrative fines were imposed by the agency. In order to obtain a judgment in a proceeding under this section, the agency shall show, following the procedures and rules of evidence as applied in ordinary civil actions, all of the following:

(1) That the administrative fines were imposed following the procedures set forth in this title and implementing regulations.

(2) That the defendant or defendants in the action were notified, by actual or constructive notice, of the imposition of the administrative fines.

(3) That a demand for payment has been made by the agency and full payment has not been received.

(b) A civil action brought pursuant to subdivision (a) shall be commenced within four years after the date on which the administrative fines were imposed.

SEC. 24.15. Section 1798.199.80 is added to the Civil Code, to read:

1798.199.80. (a) If the time for judicial review of a final agency order or decision has lapsed, or if all means of judicial review of the order or decision have been exhausted, the agency may apply to the clerk of the court for a judgment to collect the administrative fines imposed by the order or decision, or the order as modified in accordance with a decision on judicial review.

(b) The application, which shall include a certified copy of the order or decision, or the order as modified in accordance with a decision on judicial review, and proof of service of the order or decision, constitutes a sufficient showing to warrant issuance of the judgment to collect the administrative fines. The clerk of the court shall enter the judgment immediately in conformity with the application.

(c) An application made pursuant to this section shall be made to the clerk of the superior court in the county where the administrative fines were imposed by the agency.

(d) A judgment entered in accordance with this section has the same force and effect as, and is subject to all the provisions of law relating to, a judgment in a civil action and may be enforced in the

same manner as any other judgment of the court in which it is entered.

(e) The agency may bring an application pursuant to this section only within four years after the date on which all means of judicial review of the order or decision have been exhausted.

(f) The remedy available under this section is in addition to those available under any other law.

SEC. 24.16. Section 1798.199.85 is added to the Civil Code, to read:

*1798.199.85. Any decision of the agency with respect to a complaint or administrative fine shall be subject to judicial review in an action brought by an interested party to the complaint or administrative fine and shall be subject to an abuse of discretion standard.*

SEC. 24.17. Section 1798.199.90 is added to the Civil Code, to read:

*1798.199.90. (a) Any business, service provider, contractor, 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 and each violation involving the personal information of minor consumers, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185, 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 court may consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of the civil penalty.*

*(b) Any civil penalty recovered by an action brought by the Attorney General for a violation of this title, and the proceeds of any settlement of any said action, shall be deposited in the Consumer Privacy Fund.*

*(c) The agency shall, upon request by the Attorney General, stay an administrative action or investigation under this title to permit the Attorney General to proceed with an investigation or civil action and shall not pursue an administrative action or investigation, unless the Attorney General subsequently determines not to pursue an investigation or civil action. The agency may not limit the authority of the Attorney General to enforce this title.*

*(d) No civil action may be filed by the Attorney General under this section for any violation of this title after the agency has issued a decision pursuant to Section 1798.199.85 or an order pursuant to Section 1798.199.55 against that person for the same violation.*

*(e) This section shall not affect the private right of action provided for in Section 1798.150.*

SEC. 24.18. Section 1798.199.95 is added to the Civil Code, to read:

*1798.199.95. (a) There is hereby appropriated from the General Fund of the state to the agency the sum of five million dollars (\$5,000,000) during the fiscal year 2020–2021, and the sum of ten million dollars (\$10,000,000) adjusted for cost-of-living changes, during each fiscal year thereafter, for expenditure to support the operations of the agency pursuant to this title. The expenditure of funds under this appropriation shall be subject to the normal administrative review given to other state appropriations. The Legislature shall appropriate those additional amounts to the commission and other agencies as may be necessary to carry out the provisions of this title.*

*(b) The Department of Finance, in preparing the state budget and the Budget Act bill submitted to the Legislature, shall include an item for the support of this title that shall indicate all of the following:*

*(1) The amounts to be appropriated to other agencies to carry out their duties under this title, which amounts shall be in augmentation of the support items of those agencies.*

*(2) The additional amounts required to be appropriated by the Legislature to the agency to carry out the purposes of this title, as provided for in this section.*

*(3) In parentheses, for informational purposes, the continuing appropriation during each fiscal year of ten million dollars (\$10,000,000), adjusted for cost-of-living changes made pursuant to this section.*

*(c) The Attorney General shall provide staff support to the agency until the agency has hired its own staff. The Attorney General shall be reimbursed by the agency for these services.*

SEC. 24.19. Section 1798.199.100 is added to the Civil Code, to read:

*1798.199.100. The agency and any court, as applicable, shall consider the good faith cooperation of the business, service provider, contractor, or other person in determining the amount of any administrative fine or civil penalty for a violation of this title. A business shall not be required by the agency, a court, or otherwise to pay both an administrative fine and a civil penalty for the same violation.*

SEC. 25. Amendment.

*(a) The provisions of this act may be amended after its approval by the voters by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor, provided that those amendments are consistent with and further the purpose and intent of this act as set forth in Section 3, including amendments to the exemptions in Section 1798.145 if the laws upon which the exemptions are based are amended to enhance privacy and are consistent with and further*

the purposes and intent of this act and amendments to address a decision of a state or federal court holding that a provision of the act is unconstitutional or preempted by federal law, provided that any further amendments to legislation that addresses a court holding shall be subject to this subdivision.

(b) Notwithstanding Section 1798.199.25, the Legislature may authorize additional compensation for members of the California Consumer Privacy Agency, if it determines that it is necessary to carry out the agency's functions, by a statute that is passed by a vote of a majority of the members of each house of the Legislature and signed by the Governor.

(c) This section applies to all statutes amended or reenacted as part of this act, and all provisions of those statutes, regardless of whether this act makes any substantive change thereto.

(d) The provisions of this act shall prevail over any conflicting legislation enacted after January 1, 2020. Any amendments to this act or any legislation that conflicts with any provision of this act shall be null and void upon passage of this act by the voters, regardless of the code in which it appears. Legislation shall be considered "conflicting" for purposes of this subdivision, unless the legislation is consistent with and furthers the purpose and intent of this act as set forth in Section 3.

#### SEC. 26. Severability.

If any provision of this measure, or part of this measure, or the application of any provision or part to any person or circumstances, is for any reason held to be invalid, the remaining provisions, or applications of provisions, shall not be affected, but shall remain in full force and effect, and to this end the provisions of this measure are severable. If a court were to find in a final, unreviewable judgment that the exclusion of one or more entities or activities from the applicability of the act renders the act unconstitutional, those exceptions should be severed and the act should be made applicable to the entities or activities formerly exempt from the act. It is the intent of the voters that this act would have been enacted regardless of whether any invalid provision had been included or any invalid application had been made.

#### SEC. 27. Conflicting Initiatives.

(a) In the event that this measure and another measure addressing consumer privacy shall appear on the same statewide ballot, the provisions of the other measure or measures shall be deemed to be in conflict with this measure. In the event that this measure receives a greater number of affirmative votes than a measure deemed to be in conflict with it, the provisions of this measure shall prevail in their entirety, and the other measure or measures shall be null and void.

(b) If this measure is approved by the voters but superseded by law by any other conflicting measure

approved by voters at the same election, and the conflicting ballot measure is later held invalid, this measure shall be self-executing and given full force and effect.

#### SEC. 28. Standing.

Notwithstanding any other provision of law, if the state or any of its officials fail to defend the constitutionality of this act, following its approval by the voters, any other government agency of this state shall have the authority to intervene in any court action challenging the constitutionality of this act for the purpose of defending its constitutionality, whether that action is in state or federal trial court, on appeal, or on discretionary review by the Supreme Court of California or the Supreme Court of the United States. The reasonable fees and costs of defending the action shall be a charge on funds appropriated to the Department of Justice, which shall be satisfied promptly.

#### SEC. 29. Construction.

This act shall be liberally construed to effectuate its purposes.

#### SEC. 30. Savings Clause.

This act is intended to supplement federal and state law, where permissible, but shall not apply if that application is preempted by, or in conflict with, federal law, or the California Constitution. The provisions of the act relating to children under 16 years of age shall only apply to the extent not in conflict with the federal Children's Online Privacy Protection Act.

#### SEC. 31. Effective and Operative Dates.

(a) This act shall become effective as provided in subdivision (a) of Section 10 of Article II of the California Constitution. Except as provided in subdivision (b), this act shall become operative January 1, 2023, and with the exception of the right of access, shall only apply to personal information collected by a business on or after January 1, 2022.

(b) Subdivisions (m) and (n) of Section 1798.145, Sections 1798.160, 1798.185, Sections 1798.199.10 through 1798.199.40, inclusive, and Section 1798.199.95 shall become operative on the effective date of the act.

(c) The provisions of the California Consumer Privacy Act of 2018, amended by this act, shall remain in full force and effect and shall be enforceable until the same provisions of this act become operative and enforceable.

## PROPOSITION 25

This law proposed by Senate Bill 10 of the 2017-2018 Regular Session (Chapter 244, Statutes of 2018) is submitted to the people as a referendum in

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

*Exhibit 2*



**CALIFORNIA PRIVACY PROTECTION AGENCY**

**TITLE 11. LAW**

**DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY  
CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS**

**NOTICE OF PROPOSED RULEMAKING**

Notice published July 8, 2022.

The California Privacy Protection Agency (Agency) proposes to amend sections 7000, 7001, 7010, 7011, 7012, 7013, 7016, 7020, 7021, 7022, 7024, 7026, 7028, 7050, 7060, 7061, 7062, 7063, 7070, 7071, 7072, 7080, 7081, 7100, 7101, and 7102, adopt sections 7002, 7003, 7004, 7014, 7015, 7023, 7025, 7027, 7051, 7052, 7053, 7300, 7301, 7302, 7303, and 7304, and repeal section 7031 of title 11, division 6, chapter 1 of the California Code of Regulations concerning the California Consumer Privacy Act.

**PUBLIC HEARING**

The Agency will hold a public hearing to provide all interested persons an opportunity to present statements or arguments, either orally or in writing, with respect to the proposed regulations, at the following dates and time at the physical location identified below and via Zoom video and telephone conference:

**Dates:** August 24 and 25, 2022  
**Time:** 9:00 a.m. Pacific Time  
**Location:** Elihu M. Harris State Building  
1515 Clay Street  
Oakland, CA 94612  
Auditorium (1st floor)

To join this hearing by Zoom video conference:  
**<https://coppa-ca-gov.zoom.us/j/89421145939>**

Or Telephone:  
USA (216) 706-7005 US Toll  
USA (866) 434-5269 US Toll-free  
Conference code: 682962

Members of the public who wish to speak at the hearing are requested to RSVP in advance on the Agency's website at <https://coppa.ca.gov/regulations/>. Speakers will be called on in the order of the RSVP. The information provided will also help the Agency plan logistics and ensure that the hearing location can accommodate all participants who plan to attend in person.

## **WRITTEN COMMENT PERIOD**

Any interested person or their authorized representative may submit written comments relevant to the proposed regulatory action. The written comment period closes on August 23, 2022, at 5:00 p.m. Only written comments received by that time will be considered.

You may submit comments by the following means:

### **Electronic:**

Comments may be submitted electronically to [regulations@coppa.ca.gov](mailto:regulations@coppa.ca.gov). Please include "CPPA Public Comment" in the subject line.

### **Mail:**

California Privacy Protection Agency  
Attn: Brian Soublet  
2101 Arena Blvd., Sacramento, CA 95834  
(279) 895-6083

NOTE: Written and oral comments, attachments, and associated contact information (e.g., address, phone, email, etc.) become part of the public record and can be released to the public upon request.

## **AUTHORITY AND REFERENCE**

Authority: Section 1798.185, Civil Code.

Reference: Sections 1798.100, 1798.105, 1798.106, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, 1798.185, 1798.199.35, 1798.199.40, 1798.199.45, 1798.199.50, 1798.55, 1798.199.65, Civil Code.

## **INFORMATIVE DIGEST/POLICY STATEMENT OVERVIEW**

### **Summary of Existing Laws and Regulations:**

The Legislature enacted the California Consumer Privacy Act of 2018 (CCPA) in late 2018 and the statute became operative January 1, 2020. (Stats. 2018, c. 55 (Assem. Bill No. 375), § 3, eff. Jan. 1, 2019, operative Jan. 1, 2020.) The CCPA conferred new privacy rights for consumers and imposed corresponding obligations on businesses subject to it. The rights conferred to consumers include the right to know what personal information businesses are collecting about consumers and how that information is being used, sold, and shared, the right to delete personal information held by businesses, the right to stop the sale of personal information by businesses, and the right to non-discrimination in service and price when exercising privacy rights. (Civ. Code, §§ 1798.100-1798.199.)<sup>1</sup>

---

<sup>1</sup> All references are to the Civil Code unless otherwise indicated.

Subsequently, in November 2020, voters approved the Consumer Privacy Rights Act of 2020 (CPRA), amending and building on the CCPA. The CPRA amendments to the CCPA endow California residents with new rights of control over the personal information that covered businesses hold about them.<sup>2</sup> California consumers now have:

- The right to delete the personal information that a business collects from them (with specified exceptions for operational and legal necessity). (§ 1798.105.)
- The right to correct inaccurate personal information the business maintains about them. (§ 1798.106.)
- The right to know what personal information a business has collected about them, and how the business uses, sells, and shares that information. (§§ 1798.110, 1798.115, 1798.140, subds. (ad), (ah).)
- The right to opt out of the sale or sharing of their personal information. (§ 1798.120.)
- The right to limit a business's use and disclosure of sensitive personal information about them to certain business purposes. (§ 1798.121.)
- The right to non-discrimination, meaning that consumers who exercise their rights under the CCPA are entitled receive the same service and price as consumers who do not. (§ 1798.125.)

Businesses have corresponding duties. First, businesses are required to provide consumers with a number of disclosures about their business practices as it relates to their collection and use of consumers' personal information. Businesses must provide timely notice, at or before the point of collection, about the categories of personal information it will collect about the consumer, including categories of sensitive personal information; the purposes for which that information will be used; whether that information is sold or shared; and the length of time the business intends to retain that information. (§ 1798.100, subd. (a).) The business must not collect additional categories of personal information or use the personal information for purposes that are incompatible with the disclosed purpose for which the personal information was collected. (§ 1798.100, subd. (a)(1).) The businesses collection, use, retention, and sharing of the personal information must also be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processes, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes. (§ 1798.100, subd. (c).)

A business must also post a privacy policy that provides consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, sale,

---

<sup>2</sup> As amended by the CPRA, the CCPA now applies to businesses that collect personal information about California residents and that either (1) have gross revenues exceeding \$25 million a year; (2) buy, sell, or share the information of 100,000 or more consumers or households; or (3) derive 50 percent or more of their annual revenue from selling or sharing consumers' personal information. (§ 1798.140, subd. (d)(1)(A)-(C).)

sharing, and retention of personal information, as well as a description of a consumer's CCPA rights. (§ 1798.130, subd. (a)(5); see also Cal. Code Regs., tit. 11, § 7011.) If a business sells or shares personal information or uses or discloses sensitive personal information for certain purposes, the business must provide a "Do Not Sell or Share My Personal Information" link and/or "Limit the Use of My Sensitive Personal Information" link on its internet homepage, or an alternative opt-out link that allows consumers to exercise both their right to opt-out of the sale/sharing of their personal information and their right to limit the use of their sensitive personal information. (§ 1798.130, subd. (a).)

Businesses are required to make available to consumers two or more methods for submitting CCPA requests. (§ 1798.130, subd. (a)(1).) In obtaining consent from consumers, businesses are prohibited from using dark patterns, which is defined to mean a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice. (§ 1798.140, subds. (h), (l).) Businesses must respond to verifiable consumer requests within 45 to 90 days. (§ 1798.130, subd. (a)(2); see also Cal. Code Regs., tit. 11, §§ 7060-7062 (discussing verification of requests).) If a business is unable to comply completely with a request, it is still obliged to comply with the request as much as possible. For instance, if a business denies a consumer's request to know "in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA," the business must explain the basis for its denial and disclose information that is not subject to the exception. (Cal. Code Regs., tit. 11, § 7024, subd. (e).) Similarly, if a business denies a request to delete because of an exception to the CCPA, the business must still delete the consumer's personal information that is not subject to the exception and must not use the information retained for any other purpose than provided for by the exception. (*Id.*, § 7022, subd. (f).) Businesses must also ensure that individuals responsible for handling consumer requests about the businesses' privacy practices or the businesses' compliance with the CCPA are informed of all the requirements under the law and how to direct consumers to exercise their CCPA rights. (§ 1798.130, subd. (a)(6).)

There are a number of significant exceptions to the CCPA. First, the CCPA does not apply to government entities or nonprofit organizations, and excludes information that is lawfully made available to the general public, such as government records, widely distributed media, and information made available by a consumer if the consumer has not restricted the information to a specific audience. (§ 1798.140, subd. (d)(1), (v)(2).) The CCPA also contains a set of nuanced exceptions for certain categories of information—such as medical records, credit reporting, banking, and vehicle safety records—that apply when the information is governed by another privacy-protecting statute. (§ 1798.145, subds. (c), (d), (e), (g).)

The Attorney General submitted proposed regulations and supporting materials to the Office of Administrative Law for its consideration in June 2020, and the regulations became operative on August 14, 2020. (Cal. Code Regs., tit. 11, § 7000, et seq.) A set of amendments to the regulations went into effect March 15, 2021. (*Id.*, §§ 7013, 7026, 7063, 7072.)

On October 21, 2021, the Agency provided notice to the Attorney General that it was prepared to assume rulemaking responsibilities. Rulemaking authority transferred from the Attorney General to the Agency six months after that notice. (§§ 1798.185, subd. (d), 1798.199.40, subd. (b).) On May 5, 2022, the Office of Administrative Law (OAL), pursuant to Section 100 of OAL's regulations, approved the transfer of the existing CCPA regulations to Title 11, Division 6, a new

division of the California Code of Regulations that is under the jurisdiction of the Agency. (See OAL Matter No. 2022-0325-02, available at [https://cppa.ca.gov/regulations/pdf/2022032\\_02nr\\_approval.pdf](https://cppa.ca.gov/regulations/pdf/2022032_02nr_approval.pdf).)

### **Effect of the Proposed Rulemaking:**

The CPRA established a new agency, the California Privacy Protection Agency, to implement and enforce the CCPA. (§ 1798.199.10.) The Agency is directed to adopt regulations to further the purposes of the Act, including promulgating regulations on 22 specific topics. (§ 1798.185.) The proposed regulations primarily do three things: (1) update existing CCPA regulations to harmonize them with CPRA amendments to the CCPA; (2) operationalize new rights and concepts introduced by the CPRA to provide clarity and specificity to implement the law; and (3) reorganize and consolidate requirements set forth in the law to make the regulations easier to follow and understand.

More specifically, the proposed regulations:

- Establish rules defining the notified purposes for which a business can collect, use, retain, and share consumer personal information consistent with consumers' expectations. (§ 1798.185, subd. (a)(10).)
- Establish rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide under the CCPA 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. (§ 1798.185, subd. (a)(6).)
- Establish rules and procedures to facilitate and govern the submission of a consumer's request to opt-out of sale/sharing and request to limit and a business's compliance with the request, to ensure that consumers have the ability to exercise their choices without undue burden and to prevent businesses from engaging in deceptive or harassing conduct, including in retaliation against consumers for exercising their rights, while allowing businesses to inform consumers of the consequences of their decision. (§ 1798.185, subd. (a)(4).)
- Establish rules and procedures to facilitate a consumer's right to delete, correct, or obtain personal information. (§ 1798.185, subd. (a)(7).)
- Establish rules on how often and under what circumstances a consumer can request a correction; how a business responds to the request; how concerns regarding accuracy are resolved; the steps taken to prevent fraud; and the right to submit an addendum when a request to correct health information has been rejected. (§ 1798.185, subd. (a)(8).)
- Establish procedures to extend the 12-month period of disclosure of information after a verifiable consumer request pursuant to section 1798.130, subdivision (a)(2)(B). (§ 1798.185, subd. (a)(9).)

- Define the requirements and specifications for an opt-out preference signal. (§ 1798.185, subd. (a)(19)(A) & (B).)
- Establish regulations governing how businesses respond to an opt-out preference signal where the business has elected to comply with section 1798.135, subdivision (b). (§ 1798.185, subd. (a)(20).)
- Establish regulations governing the use or disclosure of a consumer's sensitive personal information. (§ 1798.185, subd. (a)(19)(C).)
- Further define and add to the business purposes for which businesses, service providers, and contractors may use personal information consistent with consumer expectations, and further define the business purposes for which service providers and contractors may combine personal information. (§ 1798.185, subd. (a)(10).)
- Identify the business purposes for which service providers and contractors may use consumers' personal information pursuant to a written contract with a business, for the service provider or contractor's own business purpose. (§ 1798.185, subd. (a)(11).)
- Establish procedures for filing complaints with the Agency (§ 1798.199.45) and procedures necessary for the Agency's administrative enforcement of the CPRA. (§ 1798.199.50).
- Define the scope and process for the exercise of the Agency's audit authority as well as the criteria for selecting those that would be subject to an audit. (§ 1798.185, subd. (a)(18).)
- Harmonize regulations governing opt-out mechanisms, notices, and other operational mechanisms to promote clarity and functionality. (§ 1798.185, subd. (a)(22).)

The Agency will not be promulgating rules on cybersecurity audits (§ 1798.185, subd. (a)(15)(A)), risk assessments (§ 1798.185, subd. (a)(15)(B)), or automated decisionmaking technology (§ 1798.185, subd. (a)(16)) at this time. These areas will be the subject of a future rulemaking and are not within the scope of this Notice of Proposed Rulemaking.

#### **Anticipated Benefits of the Proposed Regulations:**

The proposed regulations provide a number of significant benefits to Californians. Building off of the existing CCPA regulations, the proposed regulations provide comprehensive guidance to consumers, businesses, service providers, and third parties, on how to implement and operationalize new consumer privacy rights and other changes to the law introduced by the CPRA amendments to the CCPA. (Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(C)(2).) They set forth clear requirements for how businesses are to craft their methods for submitting consumer requests and obtaining consumer consent so that the consumer's choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns. (*Ibid.*) They also clearly explain that the CPRA amendments now restrict businesses from collecting, using, retaining, and sharing consumer personal information in a manner that is inconsistent with

consumer expectations, unless they obtain the consumer's explicit consent. In doing so, the regulations place the consumer in a position where they can knowingly and freely negotiate with a business over the business's use of the consumer's personal information. (*Id.*, § 3(C)(3).)

In addition, the proposed regulations set forth the requirements for an opt-out preference signal that consumers may use to easily opt-out of the sale or sharing of their personal information with all businesses that they interact with online. With the goal of strengthening consumer privacy, the regulations support innovation in pro-consumer and privacy-aware products and services and help businesses efficiently implement privacy-aware goods and services. (*Id.*, § 3(C)(1) & (5).) They take into consideration how privacy rights are being implemented in the marketplace presently and build upon the development of privacy-forward products and services.

Finally, the proposed regulations take into consideration privacy laws in other jurisdictions and implement compliance with the CCPA in such a way that it would not contravene a business's compliance with other privacy laws, such as the General Data Protection Regulation (GDPR) in Europe and consumer privacy laws recently passed in Colorado, Virginia, Connecticut, and Utah. In doing so, it simplifies compliance for businesses operating across jurisdictions and avoids unnecessary confusion for consumers who may not understand which laws apply to them.

**Comparable Federal Regulations:**

There are no existing federal regulations or statutes comparable to these proposed regulations.

**Determination of Inconsistency/Incompatibility with Existing State Regulations:**

The Agency has determined that these proposed regulations are not inconsistent or incompatible with existing State regulations. After conducting a review for any regulations that would relate to or affect this area, the Agency has concluded that these are the only regulations that concern the California Consumer Privacy Act.

**Forms Incorporated by Reference:**

None.

**Other Statutory Requirements:**

Section 1798.185, subdivision (a), requires the Agency to solicit broad public participation and adopt regulations to further the purposes of the CCPA. During its pre-rulemaking process, the Agency published an invitation for written comments, held informational sessions, and held stakeholder sessions to solicit public participation in the rulemaking process.

**DISCLOSURES REGARDING THE PROPOSED ACTION**

**The Agency's Initial Determinations:**

Mandate on local agencies or school districts: None.

Cost or savings to any state agency: No fiscal impact is anticipated on the Agency. The Agency's enforcement responsibilities are a result of the statute, and cannot commence prior to July 1, 2023. (§ 1798.185, subd. (d).) The proposed regulations do not create additional workload for the Agency.

The proposed regulations may impact the Department of Justice's (DOJ) expenditures for enforcement because DOJ is currently enforcing CCPA and maintains civil enforcement authority.

Cost to any local agency or school district which must be reimbursed in accordance with Government Code sections 17500 through 17630: None.

Other non-discretionary costs or savings imposed on local agencies: None.

Cost or savings in federal funding to the state: None.

Cost impacts on representative person or business:

The Agency estimates that the proposed regulations will have a cost impact of \$127.50 per business. This represents the labor cost of updating certain website information to comply with the proposed regulations.

Significant effect on housing costs: None.

Significant, statewide adverse economic impact directly affecting businesses, including ability to compete: The Agency has made an initial determination that that the proposed action will not have a significant, statewide adverse economic impact directly affecting businesses, including the ability of California businesses to compete with businesses in other states.

#### **Results of the Economic Impact Assessment (EIA):**

The Agency concludes that it is (1) unlikely that the proposal will create or eliminate jobs within the state, (2) unlikely that the proposal will create new businesses or eliminate existing businesses within the state, (3) unlikely that the proposal will result in the expansion of businesses currently doing business within the state.

The Agency also concludes that:

(1) The proposed regulations would benefit the health and welfare of California residents by operationalizing the CPRA amendments to the CCPA, thus ensuring California residents are afforded greater privacy protections.

(2) The proposal would not benefit worker safety because it does not regulate worker safety standards.

(3) The proposal would not benefit the state's environment because it does not change any applicable environmental standards.



**Business report requirement:** Section 7102 requires businesses collecting large amounts of personal information to annually compile and disclose certain metrics. The Agency proposes to amend section 7102 to require these businesses to additionally disclose information about requests to correct and requests to limit.

The Agency finds it is necessary for the health, safety or welfare of the people of this state that proposed section 7102, which requires a report, applies to businesses.

**Small business determination:** The Agency has determined that the proposed action affects small businesses.

## **CONSIDERATION OF ALTERNATIVES**

In accordance with Government Code section 11346.5, subdivision (a)(13), the Agency must determine that no reasonable alternative considered by the Agency or that has otherwise been identified and brought to the attention of the Agency would be more effective in carrying out the purpose for which the action is proposed or would be as effective and less burdensome to affected private persons than the proposed action or would be more cost-effective to affected private persons and equally effective in implementing the statutory policy or other provision of law.

The Agency has determined that the proposed regulations are the most effective way to operationalize the CPRA amendments to the CCPA. The regulations balance the benefits to consumers, the burden to businesses, and the purposes of the CCPA. The Agency considered two alternative approaches to the regulations and determined that they would be less effective in carrying out the purposes for which the regulations are proposed. Specific alternatives to individual regulations are discussed in detail in the Initial Statement of Reasons.

**More stringent regulatory requirement.** A more stringent regulatory alternative considers mandating more prescriptive compliance requirements, such as prescriptive methods for submitting, tracking, and responding to CCPA requests, and detailed training programs and record-keeping practices for all businesses subject to the CCPA. This requirement would be an additional requirement (beyond the proposed regulations) for potentially hundreds of thousands of California businesses and would impose substantial costs. The Agency rejects this regulatory alternative to allow flexibility to businesses in crafting their own processes in handling CCPA requests in order to ease the compliance burden for smaller businesses subject to the CCPA. Smaller businesses may not have the resources to devote additional staff to handle CCPA-related tasks and may not receive a substantial amount of CCPA requests requiring an extensive compliance program.

**Less stringent regulatory requirement.** A less stringent regulatory alternative would, among other things, allow limited exemption for GDPR-compliant firms. Limitations would be specific to areas where GDPR and CCPA conform in both standards and enforcement, subject to auditing as needed. This approach could achieve significant economies of scale in both private compliance and public regulatory costs. The Agency rejects this regulatory alternative because of key differences between the GDPR and CCPA, especially in terms of how personal information

is defined and the consumer's right to opt-out of the sale or sharing of personal information (which is not required in the GDPR).

### **CONTACT PERSONS**

Inquiries concerning the proposed administrative action may be directed to:

California Privacy Protection Agency  
Attn: Brian Soublet  
2101 Arena Blvd., Sacramento, CA 95834  
(279) 895-6083  
regulations@coppa.ca.gov

Questions regarding procedure, comments, or the substance of the proposed action should be addressed to the above contact person. In the event the contact person is unavailable, inquiries regarding the proposed action may be directed to the following backup contact person:

California Privacy Protection Agency  
Attn: Von Chitambira  
2101 Arena Blvd., Sacramento, CA 95834  
(279) 895-1412  
regulations@coppa.ca.gov

### **AVAILABILITY OF STATEMENT OF REASONS, TEXT OF PROPOSED REGULATIONS, AND RULEMAKING FILE**

The Agency will have the entire rulemaking file available for inspection and copying throughout the rulemaking process upon request to the contact person above. As of the date this Notice of Proposed Rulemaking (Notice) is published in the Notice Register, the rulemaking file consists of this Notice, the Text of Proposed Regulations (the "express terms" of the regulations), the Initial Statement of Reasons, and any information upon which the proposed rulemaking is based. The text of this Notice, the express terms, the Initial Statement of Reasons, and any information upon which the proposed rulemaking is based are available on the Agency's website at <https://coppa.ca.gov/regulations/>. Please refer to the contact information listed above to obtain copies of these documents.

### **AVAILABILITY OF CHANGED OR MODIFIED TEXT**

After the Agency analyzes all timely and relevant comments received during the 45-day public comment period, the Agency will either adopt these regulations substantially as described in this notice or make modifications based on the comments. If the Agency makes modifications which are sufficiently related to the originally-proposed text, it will make the modified text (with the changes clearly indicated) available to the public for at least 15 days before the Agency adopts the regulations as revised. Please send requests for copies of any modified regulations to the attention of the name and address indicated above. The Agency will accept written comments on the modified regulations for 15 days after the date on which they are made available.

**AVAILABILITY OF THE FINAL STATEMENT OF REASONS**

Upon its completion, a copy of the Final Statement of Reasons will be available on the Agency's website at <https://cppa.ca.gov/regulations/>. Please refer to the contact information included above to obtain a written copy of the Final Statement of Reasons.

**AVAILABILITY OF DOCUMENTS ON THE INTERNET**

Copies of the Notice of Proposed Rulemaking, the express terms, the Initial Statement of Reasons, and any information upon which the proposed rulemaking is based are available on the Agency's website at <https://cppa.ca.gov/regulations/>.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

*Exhibit 3*

**CALIFORNIA PRIVACY PROTECTION AGENCY**

**TITLE 11. LAW**

**DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY**

**CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS**

**WRITTEN JUSTIFICATION FOR EARLIER EFFECTIVE DATE  
AND REQUEST FOR EXPEDITED REVIEW**

The California Consumer Privacy Act (CCPA) was enacted in 2018 and took effect on January 1, 2020. In November 2020, voters approved the Consumer Privacy Rights Act of 2020 (CPRA), amending and building on the CCPA. The CPRA established a new agency, the California Privacy Protection Agency (Agency), to implement and enforce the CCPA. (Civ. Code § 1798.199.10.) The CPRA requires the Agency to adopt regulations to operationalize the CPRA amendments to the CCPA by **July 1, 2022**.

To prepare the proposed regulations, the Agency held preliminary rulemaking sessions online, heard from numerous stakeholder organizations, consulted with experts, conducted two days of public hearings, and reviewed over 150 written comment letters. The Notice of Proposed Rulemaking Action was published on July 8, 2022, and in an effort to expedite final regulations, the Agency is submitting its rulemaking package four and half months prior to the one-year deadline under the Administrative Procedure Act, codified at Government Code section 11346.4, subdivision (b). Once final regulations are adopted, the Agency will enforce the regulations that establish procedures to facilitate new consumer rights under the CCPA and provide guidance to businesses for how to comply. The Agency requests expedited review and that these regulations become effective upon filing with the Secretary of State.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

*Exhibit 4*

**FINAL REGULATIONS TEXT**

**CALIFORNIA PRIVACY PROTECTION AGENCY**

**TITLE 11. LAW**

**DIVISION 6. CALIFORNIA PRIVACY PROTECTION AGENCY**

**CHAPTER 1. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS**

**Article 1. GENERAL PROVISIONS**

**§ 7000. Title and Scope.**

- (a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as “these regulations.” These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.
- (b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

*Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, and 1798.185, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55 and 1798.199.65, Civil Code.*

**§ 7001. Definitions.**

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

- ~~(a) “Affirmative authorization” means an action that demonstrates the intentional decision by the consumer to opt in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a consumer under 13 years of age, it means that the parent or guardian has provided consent to the sale of the consumer’s personal information in accordance with the methods set forth in section 7070. For consumers 13 years of age and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt in and then second, separately confirm their choice to opt in.~~
- (a) “Agency” means the California Privacy Protection Agency established by Civil Code section 1798.199.10 *et seq.*
- (b) “Alternative Opt-Out Link” means the alternative opt-out link that a business may provide instead of posting the two separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links as set forth in Civil Code section 1798.135, subdivision (a)(3), and specified in section 7015.

- (c) ~~(b)~~ “Attorney General” means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.
- (d) ~~(e)~~ “Authorized agent” means a natural person or a business entity ~~registered with the Secretary of State to conduct business in California~~ that a consumer has authorized to act on their behalf subject to the requirements set forth in section 7063.
- (e) ~~(d)~~ “Categories of sources” means types or groupings of persons or entities from which a business collects personal information about consumers, described with enough particularity to provide consumers with a meaningful understanding of the type of person or entity. They may include the consumer directly, advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.
- (f) ~~(e)~~ “Categories of third parties” means types or groupings of third parties with whom the business shares personal information, described with enough particularity to provide consumers with a meaningful understanding of the type of third party. They may include advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and data brokers.
- (g) ~~(f)~~ “CCPA” means the California Consumer Privacy Act of 2018, Civil Code section 1798.100 *et seq.*
- (h) ~~(g)~~ “COPPA” means the Children’s Online Privacy Protection Act, 15 U.S.C. sections 6501 to ~~6506~~6508 and 16 Code of Federal Regulations part 312.5.
- (i) “Disproportionate effort” within the context of a business, service provider, contractor, or third party responding to a consumer request means the time and/or resources expended by the business, service provider, contractor, or third party to respond to the individualized request significantly outweighs the reasonably foreseeable impact to the consumer by not responding, taking into account applicable circumstances, such as the size of the business, service provider, contractor, or third party, the nature of the request, and the technical limitations impacting their ability to respond. For example, responding to a consumer request to know may require disproportionate effort when the personal information that is the subject of the request is not in a searchable or readily-accessible format, is maintained only for legal or compliance purposes, is not sold or used for any commercial purpose, and there is no reasonably foreseeable material impact to the consumer by not responding. In contrast, the impact to the consumer of denying a request to correct inaccurate information that the business uses and/or sells may outweigh the burden on the business, service provider, contractor, or third party in honoring the request when the reasonably foreseeable consequence of denying the request would be the denial of services or opportunities to the consumer. A business, service provider, contractor, or third party that has failed to put in place adequate processes and procedures to receive and process consumer requests in accordance with the CCPA and these regulations cannot claim that responding to a consumer’s request requires disproportionate effort.



- (j) ~~(h)~~ “Employment benefits” means retirement, health, and other benefit programs, services, or products to which consumers and their dependents or their beneficiaries receive access through the consumer’s employer.
- (k) ~~(i)~~ “Employment-related information” means personal information that is collected by the business about a natural person for the reasons identified in Civil Code section 1798.145, subdivision ~~(h)~~(1). The collection of employment-related information, including for the purpose of administering employment benefits, shall be considered a ~~b~~Business ~~p~~Purpose.
- ~~(k)~~ “Household” means a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier.
- (l) ~~(j)~~ “Financial incentive” means a program, benefit, or other offering, including payments to consumers, ~~related to~~for the collection, ~~deletion, retention, or sale, or sharing of~~ personal information. Price or service differences are types of financial incentives.
- (m) “First party” means a consumer-facing business with which the consumer intends and expects to interact.
- (n) “Frictionless manner” means a business’s processing of an opt-out preference signal that complies with the requirements set forth in section 7025, subsection (f).
- (o) “Information Practices” means practices regarding the collection, use, disclosure, sale, sharing, and retention of personal information.
- (p) “Nonbusiness” means a person or entity that does not meet the definition of a “business” as defined in Civil Code section 1798.140, subdivision (d). For example, non-profits and government entities are Nonbusinesses because “business” is defined, among other things, to include only entities “organized or operated for the profit or financial benefit of its shareholders or other owners.”
- (q) ~~(f)~~ “Notice at ~~e~~Collection” means the notice given by a business to a consumer at or before the point at which a business collects personal information from the consumer as required by Civil Code section 1798.100, subdivision (b), and specified in these regulations.
- (r) “Notice of Right to Limit” means the notice given by a business informing consumers of their right to limit the use or disclosure of the consumer’s sensitive personal information as required by Civil Code sections 1798.121 and 1798.135 and specified in these regulations.
- (s) ~~(m)~~ “Notice of ~~r~~Right to ~~e~~Opt-out of Sale/Sharing” means the notice given by a business informing consumers of their right to opt-out of the sale or sharing of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.
- (t) ~~(n)~~ “Notice of ~~f~~Financial ~~i~~ncentive” means the notice given by a business explaining each financial incentive or price or service difference as required by Civil Code section 1798.125, subdivision (b), and specified in these regulations.
- (u) “Opt-out preference signal” means a signal that is sent by a platform, technology, or mechanism, on behalf of the consumer, that communicates the consumer choice to opt-out

of the sale and sharing of personal information and that complies with the requirements set forth in section 7025, subsection (b).

(v) ~~(e)~~ “Price or service difference” means (1) any difference in the price or rate charged for any goods or services to any consumer related to the collection, retention, ~~or sale,~~ or sharing of personal information, ~~including through the use of discounts, financial payments, or other benefits or penalties,~~ or (2) any difference in the level or quality of any goods or services offered to any consumer related to the collection, retention, ~~or sale,~~ or sharing of personal information, including the denial of goods or services to the consumer.

(w) ~~(p)~~ “Privacy policy,” as referred to in Civil Code section 1798.130, subdivision (a)(5), means the statement that a business shall make available to consumers describing the business’s practices, both online and offline Information Practices, ~~regarding the collection, use, disclosure, and sale of personal information,~~ and of the rights of consumers regarding their own personal information.

(x) “Request to correct” means a consumer request that a business correct inaccurate personal information that it maintains about the consumer, pursuant to Civil Code section 1798.106.

(y) ~~(q)~~ “Request to delete” means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(z) ~~(r)~~ “Request to know” means a consumer request that a business disclose personal information that it has collected about the consumer pursuant to Civil Code sections ~~1798.100, 1798.110, or 1798.115.~~ It includes a request for any or all of the following:

- (1) Specific pieces of personal information that a business has collected about the consumer;
- (2) Categories of personal information it has collected about the consumer;
- (3) Categories of sources from which the personal information is collected;
- (4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;
- (5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and
- (6) The business or commercial purpose for collecting or selling personal information.

(aa) “Request to limit” means a consumer request that a business limit the use and disclosure of the consumer’s sensitive personal information, pursuant to Civil Code section 1798.121, subdivision (a).

(bb) ~~(s)~~ “Request to opt-in to sale/sharing” means ~~the affirmative authorization an action demonstrating that the consumer has consented to the business’s sale or sharing of that the business may sell personal information about the consumer by a parent or guardian of a consumer less than 13 years of age,~~ or by a consumer at least 13 and

~~less than 16 years of age, or by a consumer who had previously opted out of the sale of their personal information.~~

- (cc) ~~(t)~~ “Request to opt-out of sale/sharing” means a consumer request that a business ~~not~~ neither sell nor share the consumer’s personal information to third parties, pursuant to Civil Code section 1798.120, subdivision (a).
- (dd) “Right to correct” means the consumer’s right to request that a business correct inaccurate personal information that it maintains about the consumer as set forth in Civil Code section 1798.106.
- (ee) “Right to delete” means the consumer’s right to request that a business delete any personal information about the consumer that the business has collected from the consumer as set forth in Civil Code section 1798.105.
- (ff) “Right to know” means the consumer’s right to request that a business disclose personal information that it has collected, sold, or shared about the consumer as set forth in Civil Code sections 1798.110 and 1798.115.
- (gg) “Right to limit” means the consumer’s right to request that a business limit the use and disclosure of a consumer’s sensitive personal information as set forth in Civil Code section 1798.121.
- (hh) “Right to opt-out of sale/sharing” means the consumer’s right to direct a business that sells or shares personal information about the consumer to third parties to stop doing so as set forth in Civil Code section 1798.120.
- (ii) ~~(u)~~ “Signed” means that the written attestation, declaration, or permission has either been physically signed or provided electronically in accordance with the Uniform Electronic Transactions Act, Civil Code section 1633.1 *et seq.*
- (jj) ~~(v)~~ “Third-party identity verification service” means a security process offered by an independent third party that verifies the identity of the consumer making a request to the business. Third-party identity verification services are subject to the requirements set forth in Article 5 regarding ~~requests to know and requests to delete, requests to correct, or requests to know.~~
- (kk) “Unstructured” as it relates to personal information means personal information that is not organized in a pre-defined manner and could not be retrieved or organized in a pre-defined manner without disproportionate effort on behalf of the business, service provider, contractor, or third party.
- (ll) ~~(w)~~ “Value of the consumer’s data” means the value provided to the business by the consumer’s data as calculated under section 7081.
- (mm) ~~(x)~~ “Verify” means to determine that the consumer making a ~~request to know or request to delete, request to correct, or request to know~~ is the consumer about whom the business has collected information, or if that consumer is less than 13 years of age, the consumer’s parent or legal guardian.

*Note: Authority cited: Sections 1798.175 and 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130,*

1798.135, 1798.140, 1798.145, 1798.150, 1798.155, 1798.175, and 1798.185, 1798.199.40, 1798.199.45, 1798.199.50, 1798.199.55 and 1798.199.65, Civil Code.

**§ 7002. Restrictions on the Collection and Use of Personal Information.**

(a) In accordance with Civil Code section 1798.100, subdivision (c), a business's collection, use, retention, and/or sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve:

- (1) The purpose(s) for which the personal information was collected or processed, which shall comply with the requirements set forth in subsection (b); or
- (2) Another disclosed purpose that is compatible with the context in which the personal information was collected, which shall comply with the requirements set forth in subsection (c).

(b) The purpose(s) for which the personal information was collected or processed shall be consistent with the reasonable expectations of the consumer(s) whose personal information is collected or processed. The consumer's reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following:

- (1) The relationship between the consumer(s) and the business. For example, if the consumer is intentionally interacting with the business on its website to purchase a good or service, the consumer likely expects that the purpose for collecting or processing the personal information is to provide that good or service. By contrast, for example, the consumer of a business's mobile flashlight application would not expect the business to collect the consumer's geolocation information to provide the flashlight service.
- (2) The type, nature, and amount of personal information that the business seeks to collect or process. For example, if a business's mobile communication application requests access to the consumer's contact list in order to call a specific individual, the consumer who is providing their contact list likely expects that the purpose of the business's use of that contact list will be to connect the consumer with the specific contact they selected. Similarly, if a business collects the consumer's fingerprint in connection with setting up the security feature of unlocking the device using the fingerprint, the consumer likely expects that the business's use of the consumer's fingerprint is only for the purpose of unlocking their mobile device.
- (3) The source of the personal information and the business's method for collecting or processing it. For example, if the consumer is providing their personal information directly to the business while using the business's product or service, the consumer likely expects that the business will use the personal information to provide that product or service. However, the consumer may not expect that the business will use that same personal information for a different product or service offered by the business or the business's subsidiary.
- (4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information, such as in

the Notice at Collection and in the marketing materials to the consumer(s) about the business's good or service. For example, the consumer that receives a pop-up notice that the business wants to collect the consumer's phone number to verify their identity when they log in likely expects that the business will use their phone number for the purpose of verifying the consumer's identity and not for marketing purposes. Similarly, the consumer may expect that a mobile application that markets itself as a service that finds cheap gas close to the consumer will collect and use the consumer's geolocation information for that specific purpose when they are using the service.

(5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s). For example, the consumer likely expects an online retailer's disclosure of the consumer's name and address to a delivery service provider in order for that service provider to deliver a purchased product, because that service provider's involvement is apparent to the consumer. By contrast, the consumer may not expect the disclosure of personal information to a service provider if the consumer is not directly interacting with the service provider or the service provider's role in the processing is not apparent to the consumer.

(c) Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following:

(1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed, based on the factors set forth in subsection (b).

(2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information, including whether it is a Business Purpose listed in Civil Code section 1798.140, subdivisions (e)(1) through (e)(8).

(3) The strength of the link between subsection (c)(1) and subsection (c)(2). For example, a strong link exists between the consumer's expectations that the personal information will be used to provide them with a requested service at the time of collection, and the use of the information to repair errors that impair the intended functionality of that requested service. This would weigh in favor of compatibility. By contrast, for example, a weak link exists between the consumer's reasonable expectations that the personal information will be collected to provide a requested cloud storage service at the time of collection, and the use of the information to research and develop an unrelated facial recognition service.

(d) For each purpose identified in subsection (a)(1) or (a)(2), the collection, use, retention, and/or sharing of a consumer's personal information to achieve that purpose shall be reasonably necessary and proportionate. The business's collection, use, retention, and/or sharing of a consumer's personal information shall also be reasonably necessary and proportionate to achieve any purpose for which the business obtains the consumer's consent in compliance with subsection (e). Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate to

achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent, shall be based on the following:

- (1) The minimum personal information that is necessary to achieve the purpose identified in subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.
  - (2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.
  - (3) The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers considered by the business in subsection (d)(2). For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.
- (e) A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a).
- (f) A business shall not collect categories of personal information other than those disclosed in its Notice at Collection in accordance with the CCPA and section 7012. If the business intends to collect additional categories of personal information or intends to use the personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, the business shall provide a new Notice at Collection. However, any additional collecting or processing of personal information shall comply with subsection (a).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.106, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.

### **§ 7003. Requirements for Disclosures and Communications to Consumers.**

- (a) Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon.
- (b) Disclosures required under Article 2 shall also:
  - (1) Use a format that makes the disclosure readable, including on smaller screens, if applicable.
  - (2) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.

- (3) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format.
- (c) For websites, a conspicuous link required under the CCPA or these regulations shall appear in a similar manner as other similarly-posted links used by the business on its Homepage(s). For example, the business shall use a font size and color that is at least the approximate size or color as other links next to it that are used by the business on its Homepage(s).
- (d) For mobile applications, a conspicuous link shall be included in the business's privacy policy, which must be accessible through the mobile application's platform page or download page. It may also be accessible through a link within the application, such as through the application's settings menu.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.

**§ 7004. Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.**

- (a) Except as expressly allowed by the CCPA and these regulations, businesses shall design and implement methods for submitting CCPA requests and obtaining consumer consent that incorporate the following principles:
- (1) Easy to understand. The methods shall use language that is easy for consumers to read and understand. When applicable, they shall comply with the requirements for disclosures to consumers set forth in section 7003.
- (2) Symmetry in choice. The path for a consumer to exercise a more privacy-protective option shall not be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option because that would impair or interfere with the consumer's ability to make a choice. Illustrative examples follow.
- (A) It is not symmetrical when a business's process for submitting a request to opt-out of sale/sharing requires more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted out. The number of steps for submitting a request to opt-out of sale/sharing is measured from when the consumer clicks on the "Do Not Sell or Share My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.
- (B) A choice to opt-in to the sale of personal information that provides only the two choices, "Yes" and "Ask me later," is not equal or symmetrical because there is

no option to decline the opt-in. “Ask me later” implies that the consumer has not declined but delayed the decision and that the business will continue to ask the consumer to opt-in. Framing the consumer’s options in this manner impairs the consumer’s ability to make a choice. An equal or symmetrical choice could be “Yes” and “No.”

(C) A website banner that provides only the two choices when seeking the consumer’s consent to use their personal information, “Accept All” and “More Information,” or “Accept All” and “Preferences,” is not equal or symmetrical because the method allows the consumer to “Accept All” in one step, but requires the consumer to take additional steps to exercise their rights over their personal information. Framing the consumer’s options in this manner impairs the consumer’s ability to make a choice. An equal or symmetrical choice could be “Accept All” and “Decline All.”

(3) Avoid language or interactive elements that are confusing to the consumer. The methods should not use double negatives. Toggles or buttons must clearly indicate the consumer’s choice. Illustrative examples follow.

(A) Giving the choice of “Yes” or “No” next to the statement “Do Not Sell or Share My Personal Information” is a double negative and a confusing choice for a consumer.

(B) Toggles or buttons that state “on” or “off” may be confusing to a consumer and may require further clarifying language.

(C) Unintuitive placement of buttons to confirm a consumer’s choice may be confusing to the consumer. For example, it is confusing to the consumer when a business at first consistently offers choices in the order of Yes, then No, but then offers choices in the opposite order—No, then Yes—when asking the consumer something that would contravene the consumer’s expectation.

(4) Avoid choice architecture that impairs or interferes with the consumer’s ability to make a choice. Businesses should also not design their methods in a manner that would impair the consumer’s ability to exercise their choice because consent must be freely given, specific, informed, and unambiguous. Illustrative examples follow.

(A) Requiring the consumer to click through disruptive screens before they are able to submit a request to opt-out of sale/sharing is a choice architecture that impairs or interferes with the consumer’s ability to exercise their choice.

(B) Bundling choices so that the consumer is only offered the option to consent to using personal information for purposes that meet the requirements set forth in section 7002, subsection (a), together with purposes that are incompatible with the context in which the personal information was collected is a choice architecture that impairs or interferes with the consumer’s ability to make a choice. For example, a business that provides a location-based service, such as a mobile application that posts gas prices within the consumer’s location, shall not require



the consumer to consent to incompatible uses (e.g., sale of the consumer's geolocation to data brokers) together with a reasonably necessary and proportionate use of geolocation information for providing the location-based services, which does not require consent. This type of choice architecture does not allow consent to be freely given, specific, informed, or unambiguous because it requires the consumer to consent to incompatible uses in order to obtain the expected service. The business should provide the consumer a separate option to consent to the business's use of personal information that does not meet the requirements set forth in section 7002, subsection (a).

(5) Easy to execute. The business shall not add unnecessary burden or friction to the process by which the consumer submits a CCPA request. Methods should be tested to ensure that they are functional and do not undermine the consumer's choice to submit the request. Illustrative examples follow.

(A) Upon clicking the "Do Not Sell or Share My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out of sale/sharing.

(B) A business that knows of, but does not remedy, circular or broken links, and nonfunctional email addresses, such as inboxes that are not monitored or have aggressive filters that screen emails from the public, may be in violation of this regulation.

(C) Businesses that require the consumer to unnecessarily wait on a webpage as the business processes the request may be in violation of this regulation.

(b) A method that does not comply with subsection (a) may be considered a dark pattern. Any agreement obtained through the use of dark patterns shall not constitute consumer consent. For example, a business that uses dark patterns to obtain consent from a consumer to sell their personal information shall be in the position of never having obtained the consumer's consent to do so.

(c) A user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. A business's intent in designing the interface is not determinative in whether the user interface is a dark pattern, but a factor to be considered. If a business did not intend to design the user interface to subvert or impair user choice, but the business knows of and does not remedy a user interface that has that effect, the user interface may still be a dark pattern. Similarly, a business's deliberate ignorance of the effect of its user interface may also weigh in favor of establishing a dark pattern.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

## ARTICLE 2. NOTICES REQUIRED DISCLOSURES TO CONSUMERS

### § 7010. Overview of Required Notices-Disclosures.

- (a) Every business that must comply with the CCPA and these regulations shall provide a privacy policy in accordance with the CCPA and section 7011.
- (b) A business that controls the collection of a consumer's ~~collects personal information from a consumer from a consumer~~ shall provide a ~~Notice at e~~Collection in accordance with the CCPA and section 7012.
- (c) Except as set forth in section 7025, subsection (g), a ~~A~~ business that sells or shares personal information shall provide a ~~Notice of r~~Right to o~~pt-out of Sale/Sharing or the Alternative Opt-out Link~~ in accordance with the CCPA and sections 7013 and 7015.
- (d) A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide a Notice of Right to Limit or the Alternative Opt-out Link in accordance with the CCPA and sections 7014 and 7015.
- (e) A business that offers a financial incentive or price or service difference shall provide a ~~Notice of f~~Financial i~~ncentive~~ in accordance with the CCPA and section 7016.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130 and 1798.135, Civil Code.*

### § 7011. Privacy Policy.

- (a) ~~Purpose and General Principles (1)~~ The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline Information p~~Practices regarding the collection, use, disclosure, and sale of personal information. It shall also inform consumers about and of the rights of consumers they have regarding their personal information and provide any information necessary for them to exercise those rights.~~
- (b) The privacy policy shall comply with section 7003, subsections (a) and (b).
- (c) ~~(2)~~ The privacy policy shall be designed and presented in a way that is easy to read and understandable to consumers. The policy shall:
  - (A) ~~Use plain, straightforward language and avoid technical or legal jargon.~~
  - (B) ~~Use a format that makes the policy readable, including on smaller screens, if applicable.~~
  - (C) ~~Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~

~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the policy in an alternative format. (E) Be available in a format that allows a consumer to print it out as a document.~~

(d) (b) The privacy policy shall be posted online and accessible through a conspicuous link that complies with section 7003, subsections (c) and (d), using the word "privacy" on the business's website ~~h~~Homepage(s) or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers. A mobile application may include a link to the privacy policy in the application's settings menu.

(e) (e) The privacy policy shall include the following information:

(1) A comprehensive description of the business's online and offline Information Practices, which includes the following:

(A) Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described using the specific terms set forth in Civil Code section 1798.140, subdivisions (v)(1)(A) to (K) and (ae)(1) to (3). To the extent that the business has discretion in its description, the business shall describe the category in a manner that provides consumers a meaningful understanding of the information being collected.

(B) Identification of the categories of sources from which the personal information is collected.

(C) Identification of the specific business or commercial purpose for collecting personal information from consumers. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected.

(D) Identification of the categories of personal information, if any, that the business has sold or shared to third parties in the preceding 12 months. If the business has not sold or shared consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(E) For each category of personal information identified in subsection (e)(1)(D), the categories of third parties to whom the information was sold or shared.

(F) Identification of the specific business or commercial purpose for selling or sharing consumers' personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is sold or shared.

- (G) A statement regarding whether the business has actual knowledge that it sells or shares the personal information of consumers under 16 years of age.
  - (H) Identification of the categories of personal information, if any, that the business has disclosed for a business purpose to third parties in the preceding 12 months. If the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.
  - (I) For each category of personal information identified in subsection (e)(1)(H), the categories of third parties to whom the information was disclosed.
  - (J) Identification of the specific business or commercial purpose for disclosing the consumer's personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is disclosed.
  - (K) A statement regarding whether the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m).
- (2) An explanation of the rights that the CCPA confers on consumers regarding their personal information, which includes all of the following:
- (A) The right to know what personal information the business has collected about the consumer, including the categories of personal information, the categories of sources from which the personal information is collected, the business or commercial purpose for collecting, selling, or sharing personal information, the categories of third parties to whom the business discloses personal information, and the specific pieces of personal information the business has collected about the consumer.
  - (B) The right to delete personal information that the business has collected from the consumer, subject to certain exceptions.
  - (C) The right to correct inaccurate personal information that a business maintains about a consumer.
  - (D) If the business sells or shares personal information, the right to opt-out of the sale or sharing of their personal information by the business.
  - (E) If the business uses or discloses sensitive personal information for reasons other than those set forth in section 7027, subsection (m), the right to limit the use or disclosure of sensitive personal information by the business.
  - (F) The right not to receive discriminatory treatment by the business for the exercise of privacy rights conferred by the CCPA, including an employee's, applicant's, or independent contractor's right not to be retaliated against for the exercise of their CCPA rights.
- (3) An explanation of how consumers can exercise their CCPA rights and what consumers can expect from that process, which includes all of the following:

- (A) An explanation of the methods by which the consumer can exercise their CCPA rights.
  - (B) Instructions for submitting a request under the CCPA, including any links to an online request form or portal for making such a request, if offered by the business.
  - (C) If the business sells or shares personal information, and is required to provide a Notice of Right to Opt-out of Sale/Sharing, the contents of the Notice of Right to Opt-out of Sale/Sharing or a link to that notice in accordance with section 7013, subsection (f).
  - (D) If the business uses or discloses sensitive personal information for purposes other than those specified in section 7027, subsection (m), and is required to provide a Notice of Right to Limit, the contents of the Notice of Right to Limit or a link to that notice in accordance with section 7014, subsection (f).
  - (E) A general description of the process the business uses to verify a consumer request to know, request to delete, and request to correct, when applicable, including any information the consumer must provide.
  - (F) Explanation of how an opt-out preference signal will be processed for the consumer (i.e., whether the signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances) and how the consumer can use an opt-out preference signal.
  - (G) If the business processes opt-out preference signals in a frictionless manner, information on how consumers can implement opt-out preference signals for the business to process in a frictionless manner.
  - (H) Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.
  - (I) If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.
  - (J) A contact for questions or concerns about the business's privacy policies and Information Practices using a method reflecting the manner in which the business primarily interacts with the consumer.
- (4) Date the privacy policy was last updated.
- (5) If subject to the data reporting requirements set forth in section 7102, the information required under section 7102, or a link to such information.
- ~~(1) Right to Know About Personal Information Collected, Disclosed, or Sold.~~
- ~~a. Explanation that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.~~

- ~~b. Instructions for submitting a verifiable consumer request to know and links to an online request form or portal for making the request, if offered by the business.~~
- ~~c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.~~
- ~~d. Identification of the categories of personal information the business has collected about consumers in the preceding 12 months. The categories shall be described in a manner that provides consumers a meaningful understanding of the information being collected.~~
- ~~e. Identification of the categories of sources from which the personal information is collected.~~
- ~~f. Identification of the business or commercial purpose for collecting or selling personal information. The purpose shall be described in a manner that provides consumers a meaningful understanding of why the information is collected or sold.~~
- ~~g. Disclosure or Sale of Personal Information:
 
  - ~~1. Identification of the categories of personal information, if any, that the business has disclosed for a business purpose or sold to third parties in the preceding 12 months.~~
  - ~~2. For each category of personal information identified, the categories of third parties to whom the information was disclosed or sold.~~
  - ~~3. Statement regarding whether the business has actual knowledge that it sells the personal information of consumers under 16 years of age.~~~~

~~(2) Right to Request Deletion of Personal Information.~~

- ~~a. Explanation that the consumer has a right to request the deletion of their personal information collected by the business.~~
- ~~b. Instructions for submitting a verifiable consumer request to delete and links to an online request form or portal for making the request, if offered by the business.~~
- ~~c. General description of the process the business will use to verify the consumer request, including any information the consumer must provide.~~

~~(3) Right to Opt-Out of the Sale of Personal Information.~~

- ~~a. Explanation that the consumer has a right to opt-out of the sale of their personal information by a business.~~
- ~~b. Statement regarding whether or not the business sells personal information. If the business sells personal information, include either the contents of the notice of right to opt-out or a link to it in accordance with section 7013.~~

~~(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights.~~

- a. ~~Explanation that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.~~
- (5) ~~Authorized Agent.~~
  - a. ~~Instructions on how an authorized agent can make a request under the CCPA on the consumer's behalf.~~
- (6) ~~Contact for More Information.~~
  - a. ~~A contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.~~
- (7) ~~Date the privacy policy was last updated.~~
- (8) ~~If subject to the requirements set forth in section 7102, subsection (a), the information compiled in section 7102, subsection (a)(1), or a link to it.~~
- (9) ~~If the business has actual knowledge that it sells the personal information of consumers under 16 years of age, a description of the processes required by sections 7070 and 7071.~~

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, and 1798.130 and 1798.135, Civil Code.*

## **§ 7012. Notice at Collection of Personal Information.**

- (a) ~~Purpose and General Principles~~ (1) ~~The purpose of the nNotice at eCollection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them, and the purposes for which the personal information will be used. is collected or used, and whether that information is sold or shared, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. For example, upon receiving the Notice at Collection, the consumer can use the information in the notice as a tool to choose whether to engage with the business, or to direct the business not to sell or share their personal information and to limit the use and disclosure of their sensitive personal information.~~
- (2) ~~The notice at collection shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~
  - (A) ~~Use plain, straightforward language and avoid technical or legal jargon.~~
  - (B) ~~Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~
  - (C) ~~Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~

~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~

(b) The Notice at Collection shall comply with section 7003, subsections (a) and (b).

(c) ~~(3)~~ The Notice at eCollection shall be made readily available where consumers will encounter it at or before the point of collection of any personal information. Illustrative examples follow:

(1) ~~(A)~~ When a business collects consumers' personal information online, it may post a conspicuous link to the notice on the introductory page of the business's website and on all webpages where personal information is collected.

(2) When a business collects consumers' personal information through a webform, it may post a conspicuous link to the notice in close proximity to the fields in which the consumer inputs their personal information, or in close proximity to the button by which the consumer submits their personal information to the business.

(3) ~~(B)~~ When a business collects personal information through a mobile application, it may provide a link to the notice on the mobile application's download page and within the application, such as through the application's settings menu.

(4) ~~(C)~~ When a business collects consumers' personal information offline, it may include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to where the notice can be found online.

(5) ~~(D)~~ When a business collects personal information over the telephone or in person, it may provide the notice orally.

(4) ~~When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, it shall provide a just-in-time notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. For example, if the business offers a flashlight application and the application collects geolocation information, the business shall provide a just-in-time notice, such as through a pop-up window when the consumer opens the application, that contains the information required by this subsection.~~

(5) ~~A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.~~

(d) ~~(6)~~ If a business does not give the Notice at eCollection to the consumer at or before the point of collection of their personal information, the business shall not collect personal information from the consumer.



(e) (b)-A business shall include the following in its Notice at eCollection:

- (1) A list of the categories of personal information about consumers, including categories of sensitive personal information, to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.
  - (2) The business or commercial purpose(s) for which the categories of personal information, including categories of sensitive personal information, are collected will be and used.
  - (3) Whether each category of personal information identified in subsection (e)(1) is sold or shared.
  - (4) The length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will be retained.
  - (5) (3)-If the business sells or shares personal information, the link to the Notice of Right to Opt-out of Sale/Sharing titled "Do Not Sell or Share My Personal Information" required by section 7026, subsection (a), or in the case of offline notices, where the webpage can be found online.
  - (6) (4)-A link to the business's privacy policy, or in the case of offline notices, where the privacy policy can be found online.
- (f) (e)-If a business collects personal information from a consumer online, the Notice at eCollection may be given to the consumer by providing a link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (b)(e)(1) through (6). Directing the consumer to the beginning of the privacy policy, or to another section of the privacy policy that does not contain the required information, so that the consumer is required to scroll through other information in order to determine the categories of personal information to be collected and/or whether the business sells or shares the personal information collected, does not satisfy this standard.
- (g) Third Parties that Control the Collection of Personal Information. This subsection shall not affect the first party's obligations under the CCPA to comply with a consumer's request to opt-out of sale/sharing.
- (1) For purposes of giving Notice at Collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a Notice at Collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a Notice at Collection. The first party and third parties may provide a single Notice at Collection that includes the required information about their collective Information Practices.

(2) A business that, acting as a third party, controls the collection of personal information on another business's physical premises, such as in a retail store or in a vehicle, shall provide a Notice at Collection in a conspicuous manner at the physical location(s) where it is collecting the personal information.

(3) Illustrative examples follow.

(A) Business F allows Business G, a third party ad network, to collect consumers' personal information through Business F's website. Business F may post a conspicuous link to its Notice at Collection on its Homepage(s). Business G shall provide a Notice at Collection on its Homepage(s) or include the required information about its Information Practices in Business F's Notice at Collection.

(B) Business H, a coffee shop, allows Business I, a business providing Wi-Fi services, to collect personal information from consumers using Business I's services on Business H's premises. Business H may post conspicuous signage at the entrance of the store or at the point-of-sale directing consumers to where the Notice at Collection for Business H can be found online. In addition, Business I shall post its own Notice at Collection on the first webpage or other interface consumers see before connecting to the Wi-Fi services offered.

(C) Business J, a car rental business, allows Business K to collect personal information from consumers within the vehicles Business J rents to consumers. Business J may give its Notice at Collection to the consumer at the point of sale, i.e., at the rental counter, either in writing or orally. Business K may provide its own Notice at Collection within the vehicle, such as through signage on the vehicle's computer dashboard directing consumers to where the notice can be found online.

~~(h) (d) A business that does not neither collects nor controls the collection of personal information directly from the consumer does not need to provide a Notice at eCollection to the consumer if it does not neither sells nor shares the consumer's personal information.~~

~~(i) (e) A data broker registered with the Attorney General pursuant to Civil Code section 1798.99.80 et seq., where it that does not collects personal information from a source other than directly from the consumer, does not need to provide a Notice at eCollection to the consumer if it has included in its registration submission a link to its online privacy policy that includes instructions on how a consumer can submit a request to opt-out of sale/sharing.~~

~~(f) A business collecting employment-related information shall comply with the provisions of section 7012, except with regard to the following:~~

~~(1) The notice at collection of employment-related information does not need to include the link or web address to the link titled "Do Not Sell My Personal Information".~~

~~(2) The notice at collection of employment-related information is not required to provide a link to the business's privacy policy.~~

~~(g) Subsection (f) shall become inoperative on January 1, 2021, unless the CCPA is amended otherwise.~~

*Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.99.82, 1798.100, 1798.115, 1798.120, 1798.121, 1798.145 and 1798.185, Civil Code.*

**§ 7013. Notice of Right to Opt-Out of Sale/Sharing ~~of and~~ the “Do Not Sell or Share My Personal Information” Link.**

- (a) ~~Purpose and General Principles (1)~~ The purpose of the Notice of Right to Opt-out of Sale/Sharing is to inform consumers of their right to direct a business that sells or shares their personal information to stop selling or sharing their personal information and to provide them with the opportunity to exercise that right. The purpose of the “Do Not Sell or Share My Personal Information” link is to immediately effectuate the consumer’s right to opt-out of sale/sharing, or in the alternative, direct the consumer to the Notice of Right to Opt-out of Sale/Sharing. Accordingly, clicking the business’s “Do Not Sell or Share My Personal Information” link will either have the immediate effect of opting the consumer out of the sale or sharing of personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.
- (2) ~~The notice of right to opt-out shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~
- ~~(A) Use plain, straightforward language and avoid technical or legal jargon.~~
  - ~~(B) Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~
  - ~~(C) Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~
  - ~~(D) Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~
- (b) The Notice of Right to Opt-out of Sale/Sharing shall comply with section 7003, subsections (a) and (b).
- (c) The “Do Not Sell or Share My Personal Information” link shall be a conspicuous link that complies with section 7003, subsections (c) and (d) and is located at either the header or footer of the business’s internet Homepage(s).
- (d) In lieu of posting the “Do Not Sell or Share My Personal Information” link, a business may provide the Alternative Opt-out Link in accordance with section 7015 or process opt-out preference signals in a frictionless manner in accordance with section 7025, subsections (f) and (g). The business must still post a Notice of Right to Opt-out of Sale/Sharing in accordance with these regulations.
- (e) ~~(b)~~ A business that sells or shares the personal information of consumers shall provide the Notice of Right to Opt-out of Sale/Sharing to consumers as follows:

- (1) A business shall post the Notice of Right to Opt-out of Sale/Sharing on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell or Share My Personal Information" link on the website homepage or the download or landing page of a mobile application. ~~In addition, a business that collects personal information through a mobile application may provide a link to the notice within the application, such as through the application's settings menu.~~ The notice shall include the information specified in subsection (ef) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Do Not Sell or Share My Personal Information" link immediately effectuates the consumer's right to opt-out of sale/sharing or if the business processes opt-out preference signals in a frictionless manner and chooses not to post a link, the business shall provide the notice within its privacy policy.
  - (2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to opt-out of sale/sharing. That method shall comply with the requirements set forth in section 7004-subsection (a)(2).
  - (3) A business shall also provide the notice to opt-out of sale/sharing in the same manner in which it collects the personal information that it sells or shares. Illustrative examples follow.
    - (A) A business that sells or shares personal information that it collects in the course of interacting with consumers offline, such as in a brick-and-mortar store, shall also inform consumers by an offline method of their right to opt-out and provide instructions on how to submit a request to opt-out provide notice through an offline method, e.g., ~~Illustrative examples follow: (A) A business that sells personal information that it collects from consumers in a brick and mortar store may inform consumers of their right to opt-out on the paper forms that collect the personal information or by posting signage in the area where the personal information is collected directing consumers to where the notice opt-out information can be found online.~~
    - (B) A business that sells or shares personal information that it collects over the phone may shall provide notice inform consumers of their right to opt-out orally during the call when the information is collected.
- (f) ~~(e)~~ A business shall include the following in its Notice of Right to Opt-out of Sale/Sharing:
- (1) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business; and
  - (2) Instructions on how the consumer can submit a request to opt-out of sale/sharing. If notice is provided online, the notice shall include tThe interactive form by which the consumer can submit their request to opt-out of sale/sharing online, as required by section 7026, subsection (a)(1). , or if the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to opt-out of sale/sharing,; and

~~(3) Instructions for any other method by which the consumer may submit their request to opt out.~~

~~(g) (d) A business does not need to provide a Notice of Right to Opt-out of Sale/Sharing or the “Do Not Sell or Share My Personal Information” link if:~~

~~(1) It does not sell or share personal information; and~~

~~(2) It states in its privacy policy that it does not sell or share personal information.~~

~~(h) (e) A business shall not sell or share the personal information it collected during the time the business did not have a Notice of Right to Opt-out of Sale/Sharing posted unless it obtains the affirmative authorization consent of the consumer.~~

~~(f) Opt Out Icon:~~

~~(1) The following opt out icon may be used in addition to posting the notice of right to opt out, but not in lieu of any requirement to post the notice of right to opt out or a “Do Not Sell My Personal Information” link as required by Civil Code section 1798.135 and these regulations.~~



~~(2) The icon shall be approximately the same size as any other icons used by the business on its webpage.~~

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

**§ 7014. Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link.**

(a) The purpose of the Notice of Right to Limit is to inform consumers of their right to limit a business’s use and disclosure of their sensitive personal information and to provide them with the opportunity to exercise that right. The purpose of the “Limit the Use of My Sensitive Personal Information” link is to immediately effectuate the consumer’s right to limit, or in the alternative, direct the consumer to the Notice of Right to Limit. Accordingly, clicking the business’s “Limit the Use of My Sensitive Personal Information” link will either have the immediate effect of limiting the use and disclosure of the consumer’s sensitive personal information or lead the consumer to a webpage where the consumer can learn about and make that choice.

(b) The Notice of Right to Limit shall comply with section 7003, subsections (a) and (b).

(c) The “Limit the Use of My Sensitive Personal Information” link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s).

(d) In lieu of posting the “Limit the Use of My Sensitive Personal Information” link, a business may provide the Alternative Opt-out Link in accordance with section 7015. The business shall still post a Notice of Right to Limit in accordance with these regulations.

(e) A business that uses or discloses a consumer's sensitive personal information for purposes other than those specified in section 7027, subsection (m), shall provide the Notice of Right to Limit to consumers as follows:

(1) A business shall post the Notice of Right to Limit on the internet webpage to which the consumer is directed after clicking on the "Limit the Use of My Sensitive Personal Information" link. The notice shall include the information specified in subsection (f) or be a link that takes the consumer directly to the specific section of the business's privacy policy that contains the same information. If clicking on the "Limit the Use of My Sensitive Personal Information" link immediately effectuates the consumer's right to limit, the business shall provide the notice within its privacy policy.

(2) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to limit. That method shall comply with the requirements set forth in section 7003.

(f) A business shall include the following in its Notice of Right to Limit:

(1) A description of the consumer's right to limit; and

(2) Instruction on how the consumer can submit a request to limit. If notice is provided online, the notice shall include the interactive form by which the consumer can submit their request to limit online, as required by section 7027, subsection (b)(1). If the business does not operate a website, the notice shall explain the offline method by which the consumer can submit their request to limit.

(g) A business does not need to provide a Notice of Right to Limit or the "Limit the Use of My Sensitive Personal Information" link if:

(1) It only uses and discloses sensitive personal information that it collected about the consumer for the purposes specified in section 7027, subsection (m), and states so in its privacy policy; or

(2) It only collects or processes sensitive personal information without the purpose of inferring characteristics about a consumer, and states so in its privacy policy.

(h) A business shall not use or disclose sensitive personal information it collected during the time the business did not have a Notice of Right to Limit posted for purposes other than those specified in section 7027, subsection (m), unless it obtains the consent of the consumer.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135 and 1798.185, Civil Code.*

#### **§ 7015. Alternative Opt-Out Link.**

(a) The purpose of the Alternative Opt-out Link is to provide businesses the option of providing consumers with a single, clearly-labeled link that allows consumers to easily exercise both their right to opt-out of sale/sharing and right to limit, instead of posting the two separate "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information" links. The Alternative Opt-out Link shall direct the consumer to a

webpage that would inform them of both their right to opt-out of sale/sharing and right to limit and provide them with the opportunity to exercise both rights.

- (b) A business that chooses to use an Alternative Opt-out Link shall title the link, “Your Privacy Choices” or “Your California Privacy Choices,” and shall include the following opt-out icon adjacent to the title. The link shall be a conspicuous link that complies with section 7003, subsections (c) and (d), and is located at either the header or footer of the business’s internet Homepage(s). The icon shall be approximately the same size as other icons used by the business in the header or footer of its webpage.



- (c) The Alternative Opt-out Link shall direct the consumer to a webpage that includes the following information:
- (1) A description of the consumer’s right to opt-out of sale/sharing and right to limit, which shall comply with section 7003, subsections (a) and (b); and
  - (2) The interactive form or mechanism by which the consumer can submit their request to opt-out of sale/sharing and their right to limit online. The method shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.121, 1798.135 and 1798.185, Civil Code.

#### **§ 7016. Notice of Financial Incentive.**

- (a) ~~Purpose and General Principles~~ (1) ~~The purpose of the aNotice of fFinancial iIncentive is to explain to the consumer the material terms of a financial incentive or price or service difference the business is offering so that the consumer may make an informed decision about whether to participate. A business that does not offer a financial incentive or price or service difference is not required to provide a aNotice of fFinancial iIncentive.~~
- (b) The Notice of Financial Incentive shall comply with section 7003, subsections (a) and (b).
- (c) ~~(2) The aNotice of fFinancial iIncentive shall be designed and presented in a way that is easy to read and understandable to consumers. The notice shall:~~
- (A) ~~Use plain, straightforward language and avoid technical or legal jargon.~~
  - (B) ~~Use a format that draws the consumer’s attention to the notice and makes the notice readable, including on smaller screens, if applicable.~~
  - (C) ~~Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers in California.~~
  - (D) ~~Be reasonably accessible to consumers with disabilities. For notices provided online, the business shall follow generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1 of June 5, 2018, from the World Wide~~

~~Web Consortium, incorporated herein by reference. In other contexts, the business shall provide information on how a consumer with a disability may access the notice in an alternative format.~~

~~(E) Be readily available where consumers will encounter it before opting-in to the financial incentive or price or service difference. (3) If the business offers the financial incentive or price or service difference online, the notice may be given by providing a link that takes the consumer directly to the specific section of a business's privacy policy that contains the information required in subsection (b).~~

~~(d) (b) A business shall include the following in its a) Notice of f) Financial i) ncentive:~~

- ~~(1) A succinct summary of the financial incentive or price or service difference offered;~~
- ~~(2) A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;~~
- ~~(3) How the consumer can opt-in to the financial incentive or price or service difference;~~
- ~~(4) A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and~~
- ~~(5) An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:
  - ~~(A) A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and~~
  - ~~(B) A description of the method(s) the business used to calculate the value of the consumer's data.~~~~

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.*

### **ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS**

#### **§ 7020. Methods for Submitting Requests to Delete, Requests to Correct, and Requests to Know and ~~Requests to Delete.~~**

- ~~(a) A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests to delete, requests to correct, and requests to know. All other businesses shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll free telephone number. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.~~



- (b) A business that does not fit within subsection (a) shall provide two or more designated methods for submitting requests to delete, requests to correct, and requests to know. One of those methods must be a toll-free telephone number. If the business maintains an internet website, one of the methods for submitting these requests shall be through its website, such as through a webform. Other ~~Acceptable~~ methods for submitting ~~these requests to delete, requests to correct, and requests to know~~ may include, but are not limited to, ~~a toll-free phone number, a link or form available online through a business's website,~~ a designated email address, a form submitted in person, and a form submitted through the mail.
- (c) A business shall consider the methods by which it primarily interacts with consumers when determining which methods to provide for submitting requests ~~to delete, requests to correct, and requests to know and requests to delete~~. If the business interacts with consumers in person, the business shall consider providing an in-person method such as a printed form the consumer can directly submit or send by mail, a tablet or computer portal that allows the consumer to complete and submit an online form, or a telephone with which the consumer can call the business's toll-free number.
- (d) A business may use a two-step process for online requests to delete where the consumer must first, submit the request to delete and then second, separately confirm that they want their personal information deleted provided that the business otherwise complies with section 7004.
- (e) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:
- (1) Treat the request as if it had been submitted in accordance with the business's designated manner, or
  - (2) Provide the consumer with information on how to submit the request or remedy any deficiencies with the request, if applicable.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.*

**§ 7021. Timelines for Responding to Requests to Delete, Requests to Correct, and Requests to Know and Requests to Delete.**

- (a) No later than 10 business days after ~~Upon receiving a request to delete, request to correct, or request to know or a request to delete,~~ a business shall confirm receipt of the request ~~within 10 business days and~~ provide information about how the business will process the request. The information provided shall describe in general the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request. The confirmation may be given in the same manner in which the request was received. For example, if the request is made over the phone, the confirmation may be given orally during the phone call.

- (b) ~~Businesses shall respond to a requests to delete, request to correct, and request to know and requests to delete within no later than 45 calendar days after it receives the request.~~ The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If the business cannot verify the consumer within the 45-day time period, the business may deny the request. If necessary, businesses may take up to an additional 45 calendar days to respond to the consumer's request, for a maximum total of 90 calendar days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.*

**§ 7022. Requests to Delete.**

- (a) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified.
- (b) A business shall comply with a consumer's request to delete their personal information by:
- (1) ~~Permanently and completely erasing the personal information ~~on~~ from its existing systems with the exception of archived or back-up systems; (2) D, deidentifying the personal information; (3) A, or aggregating the consumer information;~~
  - (2) Notifying the business's service providers or contractors to delete from their records the consumer's personal information that they Collected pursuant to their written contract with the business, or if enabled to do so by the service provider or contractor, the business shall delete the personal information that the service provider or contractor Collected pursuant to their written contract with the business; and
  - (3) Notifying all third parties to whom the business has sold or shared the personal information to delete the consumer's personal information unless this proves impossible or involves disproportionate effort. If a business claims that notifying some or all third parties would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot notify all third parties. The business shall not simply state that notifying all third parties is impossible or would require disproportionate effort.
- (c) A service provider or contractor shall, with respect to personal information that they Collected pursuant to their written contract with the business and upon notification by the business, cooperate with the business in responding to a request to delete by doing all of the following:
- (1) Permanently and completely erasing the personal information from its existing systems except archived or back-up systems, deidentifying the personal information, or aggregating the consumer information, or enabling the business to do so.

- (2) To the extent that an exception applies to the deletion of personal information, deleting or enabling the business to delete the consumer's personal information that is not subject to the exception and refraining from using the consumer's personal information retained for any purpose other than the purpose provided for by that exception.
- (3) Notifying any of its own service providers or contractors to delete from their records in the same manner the consumer's personal information that they Collected pursuant to their written contract with the service provider or contractor.
- (4) Notifying any other service providers, contractors, or third parties that may have accessed personal information from or through the service provider or contractor, unless the information was accessed at the direction of the business, to delete the consumer's personal information unless this proves impossible or involves disproportionate effort.
- (d) ~~(e)~~ If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.
- (e) ~~(d)~~ In responding to a request to delete, a business shall inform the consumer whether or not it has complied with the consumer's request. ~~(e) If the business complies with the consumer's request, t~~The business shall also inform the consumer that it will maintain a record of the request as required by section 7030-7101, subsection ~~(b)~~(a). A business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from the business's its records.
- (f) In cases where a business denies a consumer's request to delete in whole or in part, the business shall do all of the following:
- (1) ~~Inform the consumer that it will not comply with the consumer's request and describe~~Provide to the consumer a detailed explanation of the basis for the denial, including any conflict with federal or state law, or exception to the CCPA, or factual basis for contending that compliance would be impossible or involve disproportionate effort, unless prohibited from doing so by law;
  - (2) Delete the consumer's personal information that is not subject to the exception; ~~and,~~
  - (3) Not use the consumer's personal information retained for any other purpose than provided for by that exception; and
  - (4) Instruct its service providers and contractors to delete the consumer's personal information that is not subject to the exception and to not use the consumer's personal information retained for any purpose other than the purpose provided for by that exception.

- (g) If a business that denies a consumer's request to delete sells or shares personal information and the consumer has not already made a request to opt-out of sale/sharing, the business shall ask the consumer if they would like to opt-out of the sale or sharing of their personal information and shall include either the contents of, or a link to, the Notice of Right to Opt-out of Sale/Sharing in accordance with section 7013.
- (h) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information as long as only if a global a single option to delete all personal information is also offered and more prominently presented than the other choices. A business that provides consumers the ability to delete select categories of personal information (e.g., purchase history, browsing history, voice recordings) in other contexts, however, must inform consumers of their ability to do so and direct them to how they can do so. For example, a business may provide the consumer with a link to a support page or other resource that explains consumers' data deletion options.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100~~, 1798.105, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

**§ 7023. Requests to Correct.**

- (a) For requests to correct, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 5, the business may deny the request to correct. The business shall inform the requestor that their identity cannot be verified.
- (b) In determining the accuracy of the personal information that is the subject of a consumer's request to correct, the business shall consider the totality of the circumstances relating to the contested personal information. A business may deny a consumer's request to correct if it determines that the contested personal information is more likely than not accurate based on the totality of the circumstances.
  - (1) Considering the totality of the circumstances includes, but is not limited to, considering:
    - (A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).
    - (B) How the business obtained the contested information.
    - (C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).
  - (2) If the business is not the source of the personal information and has no documentation in support of the accuracy of the information, the consumer's assertion of inaccuracy may be sufficient to establish that the personal information is inaccurate.
- (c) A business that complies with a consumer's request to correct shall correct the personal information at issue on its existing systems. The business shall also instruct all service

providers and contractors that maintain the personal information at issue pursuant to their written contract with the business to make the necessary corrections in their respective systems. Service providers and contractors shall comply with the business's instructions to correct the personal information or enable the business to make the corrections. If a business, service provider, or contractor stores any personal information that is the subject of the request to correct on archived or backup systems, it may delay compliance with the consumer's request to correct, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used.

(d) Documentation.

(1) A business shall accept, review, and consider any documentation that the consumer provides in connection with their right to correct whether provided voluntarily or as required by the business. Consumers should make a good-faith effort to provide businesses with all necessary information available at the time of the request.

(2) A business may require the consumer to provide documentation if necessary to rebut its own documentation that the personal information is accurate. In determining the necessity of the documentation requested, the business shall consider the following:

(A) The nature of the personal information at issue (e.g., whether it is objective, subjective, unstructured, sensitive, etc.).

(B) The nature of the documentation upon which the business considers the personal information to be accurate (e.g., whether the documentation is from a trusted source, whether the documentation is verifiable, etc.)

(C) The purpose for which the business collects, maintains, or uses the personal information. For example, if the personal information is essential to the functioning of the business, the business may require more documentation.

(D) The impact on the consumer. For example, if the personal information has a negative impact on the consumer, the business may require less documentation.

(3) Any documentation provided by the consumer in connection with their request to correct shall only be used and/or maintained by the business for the purpose of correcting the consumer's personal information and to comply with the record-keeping obligations under section 7101.

(4) The business shall implement and maintain reasonable security procedures and practices in maintaining any documentation relating to the consumer's request to correct.

(e) A business may delete the contested personal information as an alternative to correcting the information if the deletion of the personal information does not negatively impact the consumer, or the consumer consents to the deletion. For example, if deleting instead of correcting inaccurate personal information would make it harder for the consumer to obtain

a job, housing, credit, education, or other type of opportunity, the business shall process the request to correct or obtain the consumer's consent to delete the information.

- (f) In responding to a request to correct, a business shall inform the consumer whether it has complied with the consumer's request. If the business denies a consumer's request to correct in whole or in part, the business shall do the following:
- (1) Explain the basis for the denial, including any conflict with federal or state law, exception to the CCPA, inadequacy in the required documentation, or contention that compliance proves impossible or involves disproportionate effort.
  - (2) If a business claims that complying with the consumer's request to correct would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request. The business shall not simply state that it is impossible or would require disproportionate effort.
  - (3) If a business denies a consumer's request to correct personal information collected and analyzed concerning a consumer's health, the business shall also inform the consumer that they may provide a written statement to the business to be made part of the consumer's record per Civil Code section 1798.185, subdivision (a)(8)(D). The business shall explain to the consumer that the written statement is limited to 250 words per alleged inaccurate piece of personal information and shall include that the consumer must request that the statement be made part of the consumer's record. Upon receipt of such a statement, the business shall include it with the consumer's record.
  - (4) If the personal information at issue can be deleted pursuant to a request to delete, inform the consumer that they can make a request to delete the personal information and provide instructions on how the consumer can make a request to delete.
- (g) A business may deny a consumer's request to correct if the business has denied the consumer's request to correct the same alleged inaccuracy within the past six months of receiving the request. However, the business must treat the request to correct as new if the consumer provides new or additional documentation to prove that the information at issue is inaccurate.
- (h) A business may deny a request to correct if it has a good-faith, reasonable, and documented belief that a request to correct is fraudulent or abusive. The business shall inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive.
- (i) Where the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business may provide the consumer with the name of the source from which the business received the alleged inaccurate information.

(j) Upon request, a business shall disclose specific pieces of personal information that the business maintains and has collected about the consumer to allow the consumer to confirm that the business has corrected the inaccurate information that was the subject of the consumer's request to correct. This disclosure shall not be considered a response to a request to know that is counted towards the limitation of two requests within a 12-month period as set forth in Civil Code section 1798.130, subdivision (b). With regard to a correction to a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics, a business shall not disclose this information, but may provide a way to confirm that the personal information it maintains is the same as what the consumer has provided.

(k) Whether a business, service provider, or contractor has implemented measures to ensure that personal information that is the subject of a request to correct remains corrected factors into whether that business, service provider, or contractor has complied with a consumer's request to correct in accordance with the CCPA and these regulations. For example, a business, service provider, or contractor may supplement personal information it maintains about consumers with information obtained from a data broker. Failing to consider and address the possibility that corrected information may be overridden by inaccurate information subsequently received from a data broker may factor into whether that business, service provider, or contractor has adequately complied with a consumer's request to correct.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.106, 1798.130, 1798.185 and 1798.81.5, Civil Code.

#### **§ 7024. Requests to Know.**

- (a) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (b).
- (b) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 5, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business information practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.

- (c) In responding to a request to know, a business is not required to search for personal information if all of the following conditions are met:
- (1) The business does not maintain the personal information in a searchable or reasonably accessible format;
  - (2) The business maintains the personal information solely for legal or compliance purposes;
  - (3) The business does not sell the personal information and does not use it for any commercial purpose; and,
  - (4) The business describes to the consumer the categories of records that may contain personal information that it did not search because it meets the conditions stated above.
- (d) A business shall not disclose in response to a request to know a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, security questions and answers, or unique biometric data generated from measurements or technical analysis of human characteristics. The business shall, however, inform the consumer with sufficient particularity that it has collected the type of information. For example, a business shall respond that it collects "unique biometric data including a fingerprint scan" without disclosing the actual fingerprint scan data.
- (e) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial, unless prohibited from doing so by law. If the request is denied only in part, the business shall disclose the other information sought by the consumer.
- (f) A business shall use reasonable security measures when transmitting personal information to the consumer.
- (g) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 5.
- (h) In response to a request to know, a business shall provide all the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort, or the consumer requests data for a specific time period. That information shall include any personal information that the business's service providers or contractors Collected pursuant to their written contract with the business. If a business claims that providing personal information beyond the 12-month



period would be impossible or would involve disproportionate effort, the business shall provide the consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot provide personal information beyond the 12-month period. The business shall not simply state that it is impossible or would require disproportionate effort. Unless otherwise specified by the business to cover a longer period of time, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130, subdivision (a)(2), shall run from the date the business receives the request, regardless of the time required to verify the request.

(i) A service provider or contractor shall provide assistance to the business in responding to a verifiable consumer request to know, including by providing the business the consumer's personal information it has in its possession that it Collected pursuant to their written contract with the business, or by enabling the business to access that personal information.

(j) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general Information Practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(k) In responding to a verified request to know categories of personal information, the business shall provide all of the following:

- (1) The categories of personal information the business has collected about the consumer in the preceding 12 months;
- (2) The categories of sources from which the personal information was collected;
- (3) The business or commercial purpose for which it collected or sold the personal information;
- (4) The categories of third parties with whom the business shares personal information;
- (5) The categories of personal information that the business sold in the preceding 12 months, and for each category identified, the categories of third parties to whom it sold that particular category of personal information; and
- (6) The categories of personal information that the business disclosed for a business purpose in the preceding 12 months, and for each category identified, the categories of third parties to whom it disclosed that particular category of personal information.

(l) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140 and 1798.185, Civil Code.*

**§ 7025. Opt-Out Preference Signals.**

- (a) The purpose of an opt-out preference signal is to provide consumers with a simple and easy-to-use method by which consumers interacting with businesses online can automatically exercise their right to opt-out of sale/sharing. Through an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online without having to make individualized requests with each business.
- (b) A business that sells or shares personal information shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing:
- (1) The signal shall be in a format commonly used and recognized by businesses. An example would be an HTTP header field or JavaScript object.
  - (2) The platform, technology, or mechanism that sends the opt-out preference signal shall make clear to the consumer, whether in its configuration or in disclosures to the public, that the use of the signal is meant to have the effect of opting the consumer out of the sale and sharing of their personal information. The configuration or disclosure does not need to be tailored only to California or to refer to California.
- (c) When a business that collects personal information from consumers online receives or detects an opt-out preference signal that complies with subsection (b):
- (1) The business shall treat the opt-out preference signal as a valid request to opt-out of sale/sharing submitted pursuant to Civil Code section 1798.120 for that browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles. If known, the business shall also treat the opt-out preference signal as a valid request to opt-out of sale/sharing for the consumer. This is not required for a business that does not sell or share personal information.
  - (2) The business shall not require a consumer to provide additional information beyond what is necessary to send the signal. However, a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer's request to opt-out of sale/sharing. Any information provided by the consumer shall not be used, disclosed, or retained for any purpose other than processing the request to opt-out of sale/sharing. For example, a business may give the consumer the option to provide information that identifies the consumer so that the request to opt-out of sale/sharing can apply to offline sale or sharing of personal information. However, if the consumer does not respond, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device, including pseudonymous profiles.
  - (3) If the opt-out preference signal conflicts with a consumer's business-specific privacy setting that allows the business to sell or share their personal information, the business

shall process the opt-out preference signal as a valid request to opt-out of sale/sharing, but may notify the consumer of the conflict and provide the consumer with an opportunity to consent to the sale or sharing of their personal information. The business shall comply with section 7004 in obtaining the consumer's consent to the sale or sharing of their personal information. If the consumer consents to the sale or sharing of their personal information, the business may ignore the opt-out preference signal for as long as the consumer is known to the business.

- (4) If the opt-out preference signal conflicts with the consumer's participation in a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business may notify the consumer that processing the opt-out preference signal as a valid request to opt-out of sale/sharing would withdraw the consumer from the financial incentive program and ask the consumer to affirm that they intend to withdraw from the financial incentive program. If the consumer affirms that they intend to withdraw from the financial incentive program, the business shall process the consumer's request to opt-out of sale/sharing. If the business asks and the consumer does not affirm their intent to withdraw, the business may ignore the opt-out preference signal with respect to that consumer's participation in the financial incentive program for as long as the consumer is known to the business. If the business does not ask the consumer to affirm their intent with regard to the financial incentive program, the business shall still process the opt-out preference signal as a valid request to opt-out of sale/sharing for that browser or device and any consumer profile the business associates with that browser or device.
- (5) Where the consumer is known to the business, the business shall not interpret the absence of an opt-out preference signal after the consumer previously sent an opt-out preference signal as consent to opt-in to the sale or sharing of personal information.
- (6) A business may display whether it has processed the consumer's opt-out preference signal as a valid request to opt-out of sale/sharing on its website. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser, device, or consumer using an opt-out preference signal visits the website, or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.
- (7) Illustrative examples follow.

  - (A) Caleb visits Business N's website using a browser with an opt-out preference signal enabled, but he is not otherwise logged into his account and the business cannot otherwise associate Caleb's browser with a consumer profile the business maintains. Business N collects and shares Caleb's personal information tied to his browser identifier for cross-contextual advertising. Upon receiving the opt-out preference signal, Business N shall stop selling and sharing Caleb's information linked to Caleb's browser identifier for cross-contextual advertising, but it would not be able to apply the request to opt-out of the sale/sharing to Caleb's account information because the connection between Caleb's browser and Caleb's account is not known to the business.

- (B) Noelle has an account with Business O, an online retailer who manages consumer's privacy choices through a settings menu. Noelle's privacy settings default to allowing Business O to sell and share her personal information with the business's marketing partners. Noelle enables an opt-out preference signal on her browser and then visits Business O's website. Business O recognizes that Noelle is visiting its website because she is logged into her account. Upon receiving Noelle's opt-out preference signal, Business O shall treat the signal as a valid request to opt-out of sale/sharing and shall apply it to her device and/or browser and also to her account and any offline sale or sharing of personal information. Business O may inform Noelle that her opt-out preference signal differs from her current privacy settings and provide her with an opportunity to consent to the sale or sharing of her personal information, but it must process the request to opt-out of sale/sharing unless Noelle instructs otherwise. Business O must also wait at least 12 months before asking Noelle to opt-in to the sale or sharing of her personal information in accordance with section 7026, subsection (k). In addition, Business O's notification would not allow it to fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1), because it would not be complying with the requirements set forth in subsection (f).
- (C) Angela also has an account with Business O and has enabled an opt-out preference signal on her browser while logged into her account. Business O applies the opt-out preference signal as a valid request to opt-out of sale/sharing not only to Angela's current browser, but also to Angela's account because she is known to the business while making the request. Angela later logs into her account with Business O using a different device that does not have the opt-out preference signal enabled. Business O shall not interpret the absence of the opt-out preference signal as consent to opt-in to the sale of personal information.
- (D) Ramona participates in Business P's financial incentive program where she receives coupons in exchange for allowing the business to pseudonymously track and share her online browsing habits to marketing partners. Ramona enables an opt-out preference signal on her browser and then visits Business P's website. Business P knows that it is Ramona through a cookie that has been placed on her browser, but also detects the opt-out preference signal. Business P may ignore the opt-out preference signal and notify Ramona that her opt-out preference signal conflicts with her participation in the financial incentive program and ask whether she intends to withdraw from the financial incentive program. If Ramona does not affirm her intent to withdraw, Business P may ignore the opt-out preference signal and place Ramona on a whitelist so that Business P does not have to notify Ramona of the conflict again.
- (E) Ramona clears her cookies and revisits Business P's website with the opt-out preference signal enabled. Business P no longer knows that it is Ramona visiting its website. Business P shall honor Ramona's opt-out preference signal as it pertains to her browser or device and any consumer profile the business associates with that browser or device.

- (d) The business and the platform, technology, or mechanism that sends the opt-out preference signal shall not use, disclose, or retain any personal information collected from the consumer in connection with the sending or processing the request to opt-out of sale/sharing for any purpose other than sending or processing the opt-out preference signal.
- (e) Civil Code section 1798.135, subdivisions (b)(1) and (3), provides a business the choice between (1) processing opt-out preference signals and providing the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link; or (2) processing opt-out preference signals in a frictionless manner in accordance with these regulations and not having to provide the “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links or the Alternative Opt-out Link. It does not give the business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signals, though it may do so in a non-frictionless manner. If a business processes opt-out preference signals in a frictionless manner in accordance with subsections (f) and (g) of this regulation, then it may, but is not required to, provide the above-referenced links.
- (f) Except as allowed by these regulations, processing an opt-out preference signal in a frictionless manner as required by Civil Code section 1798.135, subdivision (b)(1), means that the business shall not:
- (1) Charge a fee or require any valuable consideration if the consumer uses an opt-out preference signal.
  - (2) Change the consumer’s experience with the product or service offered by the business. For example, the consumer who uses an opt-out preference signal shall have the same experience with regard to how the business’s product or service functions compared to a consumer who does not use an opt-out preference signal.
  - (3) Display a notification, pop-up, text, graphic, animation, sound, video, or any interstitial content in response to the opt-out preference signal. A business’s display of whether the consumer visiting their website has opted out of the sale or sharing their personal information shall not be in violation of this regulation. The business may also provide a link to a privacy settings page, menu, or similar interface that enables the consumer to consent to the business ignoring the opt-out preference signal with respect to the business’s sale or sharing of the consumer’s personal information provided that it complies with subsections (f)(1) through (3).
- (g) A business meeting the requirements of Civil Code section 1798.135, subdivision (b)(1) is not required to post the “Do Not Sell or Share My Personal Information” link or the Alternative Opt-out Link if it meets all of the following additional requirements:
- (1) Processes the opt-out preference signal in a frictionless manner in accordance with the CCPA and these regulations.
  - (2) Includes in its privacy policy the following information:

- (A) A description of the consumer's right to opt-out of the sale or sharing of their personal information by the business;
  - (B) A statement that the business processes opt-out preference signals in a frictionless manner;
  - (C) Information on how consumers can implement opt-out preference signals for the business to process in frictionless manner; and
  - (D) Instructions for any other method by which the consumer may submit a request to opt-out of sale/sharing.
- (3) Allows the opt-out preference signal to fully effectuate the consumer's request to opt-out of sale/sharing. For example, if the business sells or shares personal information offline and needs to request from the consumer additional information that is not provided by the opt-out preference signal in order to apply the request to opt-out of sale/sharing to offline sales and sharing of personal information, then the business has not fully effectuated the consumer's request to opt-out of sale/sharing. Illustrative examples follow.
- (A) Business Q collects consumers' online browsing history and shares it with third parties for cross-contextual advertising purposes. Business Q also sells consumers' personal information offline to marketing partners. Business Q cannot fall within the exception set forth in Civil Code section 1798.135, subdivision (b)(1) because a consumer's opt-out preference signal would only apply to Business Q's online sharing of personal information about the consumer's browser or device; the consumer's opt-out preference signal would not apply to Business Q's offline selling of the consumer's information because Business Q could not apply it to the offline selling without additional information provided by the consumer, i.e., the logging into an account.
  - (B) Business R only sells and shares personal information online for cross-contextual advertising purposes. Business R may use the exception set forth in Civil Code section 1798.135, subdivision (b)(1) and not post the "Do Not Sell or Share My Personal Information" link because a consumer using an opt-out preference signal would fully effectuate their right to opt-out of the sale or sharing of their personal information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.

**§ 7026. Requests to Opt-Out of Sale/Sharing.**

- (a) A business that sells or shares personal information shall provide two or more designated methods for submitting requests to opt-out of sale/sharing, including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," on the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll free phone number, a designated email

~~address, a form submitted in person, a form submitted through the mail, and user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.~~ (b) A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sells personal information that it makes available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt-out of sale/sharing. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

~~(1) (e) If a business that collects personal information from consumers online, the business shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods—an interactive form accessible via the “Do Not Sell or Share My Personal Information” link, the Alternative Opt-out Link, or the business’s privacy policy if the business processes an opt-out preference signal in a frictionless manner. treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer’s choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.~~ (1) Any privacy control developed in accordance with these regulations shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information. (2) If a global privacy control conflicts with a consumer’s existing business-specific privacy setting or their participation in a business’s financial incentive program, the business shall respect the global privacy control but may notify the consumer of the conflict and give the consumer the choice to confirm the business-specific privacy setting or participation in the financial incentive program.

~~(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to opt-out of sale/sharing in addition to the opt-out preference signal.~~

~~(3) Other methods for submitting requests to opt-out of the sale/sharing include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.~~

~~(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to opt-out of sale/sharing because cookies concern the collection of personal information and not the sale or sharing of personal information. An acceptable method for submitting requests to opt-out of sale/sharing must address the sale and sharing of personal information.~~

~~(b) (h) A business’s methods for submitting requests to opt-out of sale/sharing shall be easy for consumers to execute, and shall require minimal steps, and shall comply with section 7004 to allow the consumer to opt-out. A business shall not use a method is designed with the~~

purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out. Illustrative examples follow:

- ~~(1) The business's process for submitting a request to opt-out shall not require more steps than that business's process for a consumer to opt-in to the sale of personal information after having previously opted-out. The number of steps for submitting a request to opt-out is measured from when the consumer clicks on the "Do Not Sell My Personal Information" link to completion of the request. The number of steps for submitting a request to opt-in to the sale of personal information is measured from the first indication by the consumer to the business of their interest to opt-in to completion of the request.~~
- ~~(2) A business shall not use confusing language, such as double negatives (e.g., "Don't Not Sell My Personal Information"), when providing consumers the choice to opt-out.~~
- ~~(3) Except as permitted by these regulations, a business shall not require consumers to click through or listen to reasons why they should not submit a request to opt-out before confirming their request.~~
- ~~(4) The business's process for submitting a request to opt-out shall not require the consumer to provide personal information that is not necessary to implement the request.~~
- ~~(5) Upon clicking the "Do Not Sell My Personal Information" link, the business shall not require the consumer to search or scroll through the text of a privacy policy or similar document or webpage to locate the mechanism for submitting a request to opt-out.~~

(c) A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information beyond what is necessary to direct the business not to sell or share the consumer's personal information.

(d) ~~(g)~~ A business shall not require request to opt-out need not be a verifiable consumer request for a request to opt-out of sale/sharing. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer whose information shall cease to be sold or shared by the business. However, to the extent that the business can comply with a request to opt-out of sale/sharing without additional information, it shall do so.

(e) If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out of sale/sharing is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.

(f) ~~(e)~~ A business shall comply with a request to opt-out of sale/sharing by:

- (1) Ceasing to sell to and/or share with third parties the consumer's personal information as soon as feasibly possible, but no later than 15 business days from the date the business receives the request. Service providers or contractors Collecting personal information



pursuant to the written contract with the business required by the CCPA and these regulations does not constitute a sale or sharing of personal information. If a business sells a consumer's personal information to any third parties after the consumer submits their request but before the business complies with that request, it shall notify those third parties that the consumer has exercised their right to opt-out and shall direct those third parties not to sell that consumer's information.

(2) Notifying all third parties to whom the business has sold or shared the consumer's personal information, after the consumer submits the request to opt-out of sale/sharing and before the business complies with that request, that the consumer has made a request to opt-out of sale/sharing and directing them to comply with the consumer's request and forward the request to any other person to whom the third party has made the personal information available during that time period.

(g) A business may provide a means by which the consumer can confirm that their request to opt-out of sale/sharing has been processed by the business. For example, the business may display on its website "Consumer Opted Out of Sale/Sharing" or display through a toggle or radio button that the consumer has opted out of the sale of their personal information.

(h) ~~(d)~~ In responding to a request to opt-out of sale/sharing, a business may present the consumer with the choice to opt-out of the sale or sharing for certain uses of personal information for certain uses as long as a global single option to opt-out of the sale or sharing of all personal information is also offered more prominently presented than the other choices. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

(i) A business that responds to a request to opt-out of sale/sharing by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response. However, doing so in response to an opt-out preference signal will prevent the business from using the exception set forth in Civil Code section 1798.135, subdivision (b)(1).

(j) ~~(f)~~ A consumer may use an authorized agent to submit a request to opt-out of sale/sharing on the consumer's behalf if the consumer provides the authorized agent written permission signed by the consumer. A business may deny a request from an authorized agent if the agent ~~cannot~~ does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf. The requirement to obtain and provide written permission from the consumer does not apply to requests made by an opt-out preference signal. User-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(k) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request before asking a consumer who has opted out of the sale or sharing of their personal information to consent to the sale or sharing of their personal information.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140 and 1798.185, Civil Code.*

**§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.**

(a) The unauthorized use or disclosure of sensitive personal information creates a heightened risk of harm for the consumer. The purpose of the request to limit is to give consumers meaningful control over how their sensitive personal information is collected, used, and disclosed. It gives the consumer the ability to limit the business's use of sensitive personal information to that which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services, with some narrowly tailored exceptions, which are set forth in subsection (m). Sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to requests to limit.

(b) A business that uses or discloses sensitive personal information for purposes other than those set forth in subsection (m) shall provide two or more designated methods for submitting requests to limit. A business shall consider the methods by which it interacts with consumers, the manner in which the business collects the sensitive personal information that it uses for purposes other than those set forth in subsection (m), available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to limit. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer. Illustrative examples follow.

(1) A business that collects sensitive personal information from consumers online shall, at a minimum, allow consumers to submit requests to limit through an interactive form accessible via the "Limit the Use of My Sensitive Personal Information" link or the Alternative Opt-out Link.

(2) A business that interacts with consumers in person and online may provide an in-person method for submitting requests to limit in addition to the online form.

(3) Other methods for submitting requests to limit include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, and a form submitted through the mail.

(4) A notification or tool regarding cookies, such as a cookie banner or cookie controls, is not by itself an acceptable method for submitting requests to limit because cookies concern the collection of personal information and not necessarily the use and disclosure of sensitive personal information. An acceptable method for submitting requests to limit must address the specific right to limit.

- (c) A business's methods for submitting requests to limit shall be easy for consumers to execute, shall require minimal steps, and shall comply with section 7004.
- (d) A business shall not require a consumer submitting a request to limit to create an account or provide additional information beyond what is necessary to direct the business to limit the use or disclosure of the consumer's sensitive personal information.
- (e) A business shall not require a verifiable consumer request for a request to limit. A business may ask the consumer for information necessary to complete the request, such as information necessary to identify the consumer to whom the request should be applied. However, to the extent that the business can comply with a request to limit without additional information, it shall do so.
- (f) If a business has a good-faith, reasonable, and documented belief that a request to limit is fraudulent, the business may deny the request. The business shall inform the requestor that it will not comply with the request and shall provide to the requestor an explanation why it believes the request is fraudulent.
- (g) A business shall comply with a request to limit by:
- (1) Ceasing to use and disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (m) as soon as feasibly possible, but no later than 15 business days from the date the business receives the request.
  - (2) Notifying all the business's service providers or contractors that use or disclose the consumer's sensitive personal information for purposes other than those set forth in subsection (m) that the consumer has made a request to limit and instructing them to comply with the consumer's request to limit within the same time frame.
  - (3) Notifying all third parties to whom the business has disclosed or made available the consumer's sensitive personal information for purposes other than those set forth in subsection (m), after the consumer submitted their request and before the business complied with that request, that the consumer has made a request to limit and direct them 1) to comply with the consumer's request and 2) to forward the request to any other person with whom the person has disclosed or shared the sensitive personal information during that time period.
- (h) A business may provide a means by which the consumer can confirm that their request to limit has been processed by the business. For example, the business may display through a toggle or radio button that the consumer has limited the business's use and sale of their sensitive personal information.
- (i) In responding to a request to limit, a business may present the consumer with the choice to allow specific uses for the sensitive personal information as long as a single option to limit the use of the personal information is also offered.
- (j) A consumer may use an authorized agent to submit a request to limit on the consumer's behalf if the consumer provides the authorized agent written permission signed by the

consumer. A business may deny a request from an authorized agent if the agent does not provide to the business the consumer's signed permission demonstrating that they have been authorized by the consumer to act on the consumer's behalf.

- (k) A business that responds to a request to limit by informing the consumer of a charge for the use of any product or service shall comply with Article 7 and shall provide the consumer with a Notice of Financial Incentive that complies with section 7016 in its response.
- (l) Except as allowed by these regulations, a business shall wait at least 12 months from the date the consumer's request to limit is received before asking a consumer who has exercised their right to limit to consent to the use or disclosure of their sensitive personal information for purposes other than those set forth in subsection (m).
- (m) The purposes identified in Civil Code section 1798.121, subdivision (a), for which a business may use or disclose sensitive personal information without being required to offer consumers a right to limit are as follows. A business that only uses or discloses sensitive personal information for these purposes, provided that the use or disclosure is reasonably necessary and proportionate for those purposes, is not required to post a Notice of Right to Limit or provide a method for submitting a request to limit.

  - (1) To perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services. For example, a consumer's precise geolocation may be used by a mobile application that is providing the consumer with directions on how to get to specific location. A consumer's precise geolocation may not, however, be used by a gaming application where the average consumer would not expect the application to need this piece of sensitive personal information.
  - (2) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information. For example, a business may disclose a consumer's log-in information to a data security company that it has hired to investigate and remediate a data breach that involved that consumer's account.
  - (3) To resist malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those actions. For example, a business may use information about a consumer's ethnicity and/or the contents of email and text messages to investigate claims of racial discrimination or hate speech.
  - (4) To ensure the physical safety of natural persons. For example, a business may disclose a consumer's geolocation information to law enforcement to investigate an alleged kidnapping.
  - (5) For short-term, transient use, including, but not limited to, nonpersonalized advertising shown as part of a consumer's current interaction with the business, provided that the personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business. For example, a business that sells religious books can use information about its customers' interest in its religious content to serve

contextual advertising for other kinds of religious merchandise within its store or on its website, so long as the business does not use sensitive personal information to create a profile about an individual consumer or disclose personal information that reveals consumers' religious beliefs to third parties.

- (6) To perform services on behalf of the business. For example, a business may use information for maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.
- (7) To verify or maintain the quality or safety of a product, 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 by, manufactured for, or controlled by the business. For example, a car rental business may use a consumer's driver's license for the purpose of testing that its internal text recognition software accurately captures license information used in car rental transactions.
- (8) To collect or process sensitive personal information where such collection or processing is not for the purpose of inferring characteristics about a consumer. For example, a business that includes a search box on their website by which consumers can search for articles related to their health condition may use the information provided by the consumer for the purpose of providing the search feature without inferring characteristics about the consumer.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.121, 1798.135, 1798.140 and 1798.185, Civil Code.*

**§ 7028. Requests to Opt-In After Opting-Out of the Sale or Sharing of Personal Information.**

- (a) Requests to opt-in to ~~the sale or sharing~~ of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.
- (b) If a consumer who has opted-out of the sale or sharing of their personal information initiates a transaction or attempts to use a product or service that requires the sale or sharing of their personal information, ~~a the~~ business may inform the consumer that the transaction, product, or service requires the sale of their personal information and provide instructions on how the consumer can provide consent to opt-in to the sale or sharing of their personal information. The business shall comply with section 7004 when obtaining the consumer's consent.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

**~~§ 7031 Requests to Know or Delete Household Information.~~**

- ~~(a) Where a household does not have a password-protected account with a business, a business shall not comply with a request to know specific pieces of personal information about the household or a request to delete household personal information unless all of the following conditions are satisfied:~~
- ~~(1) All consumers of the household jointly request to know specific pieces of information for the household or the deletion of household personal information;~~
  - ~~(2) The business individually verifies all the members of the household subject to the verification requirements set forth in section 7062; and~~
  - ~~(3) The business verifies that each member making the request is currently a member of the household.~~
- ~~(b) Where a consumer has a password-protected account with a business that collects personal information about a household, the business may process requests to know and requests to delete relating to household information through the business's existing business practices and in compliance with these regulations.~~
- ~~(c) If a member of a household is a consumer under the age of 13, a business must obtain verifiable parental consent before complying with a request to know specific pieces of information for the household or the deletion of household personal information pursuant to the parental consent provisions in section 7070.~~

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140 and 1798.185, Civil Code.*

**ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES**

**§ 7050. § 7051. Service Providers and Contractors.**

- ~~(a) A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, shall be deemed a service provider for purposes of the CCPA and these regulations.~~
- ~~(b) To the extent that a business directs a second entity to collect personal information directly from a consumer, or about a consumer, on the first business's behalf, and the second entity would otherwise meet the requirements and obligations of a "service provider" under the CCPA and these regulations, the second entity shall be deemed a service provider of the first business for purposes of the CCPA and these regulations.~~
- ~~(a) (e) A service provider or contractor shall not retain, use, or disclose personal information Collected pursuant to its written contract with the business obtained in the course of providing services except:~~

~~(1) To process or maintain personal information on behalf of the business that provided the personal information or directed the service provider to collect the personal information~~

(1) For the specific Business Purpose(s) set forth in, and in compliance with the written contract between the business and the service provider or contractor that is for services required by the CCPA and these regulations.;

(2) To retain and employ another service provider or contractor as a subcontractor, where the subcontractor meets the requirements for a service provider or contractor under the CCPA and these regulations.;

(3) For internal use by the service provider or contractor to build or improve the quality of its the services it is providing to the business, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations, provided that the service provider or contractor use does not use the personal information to perform services on behalf of another person include building or modifying household or consumer profiles to use in providing services to another business, or correcting or augmenting data acquired from another source;. Illustrative examples follow.

(A) An email marketing service provider can send emails on a business's behalf using the business's customer email list. The service provider could analyze those customers' interactions with the marketing emails to improve its services and offer those improved services to everyone. But the service provider cannot use the original email list to send marketing emails on behalf of another business.

(B) A shipping service provider that delivers businesses' products to their customers may use the addresses received from their business clients and their experience delivering to those addresses to identify faulty or incomplete addresses, and thus, improve their delivery services. However, the shipping service provider cannot compile the addresses received from one business to send advertisements on behalf of another business, or compile addresses received from businesses to sell to data brokers.

(4) To prevent, detect, or investigate data security incidents or protect against malicious, deceptive, fraudulent or illegal activity, even if this Business Purpose is not specified in the written contract required by the CCPA and these regulations.; ~~or~~

(5) For the purposes enumerated in Civil Code section 1798.145, subdivisions (a)(1) through (a)(74).

(b) A service provider or contractor cannot contract with a business to provide cross-contextual behavioral advertising. Per Civil Code section 1798.140, subdivision (e)(6), a service provider or contractor may contract with a business to provide advertising and marketing services, but the service provider or contractor shall not combine the personal information of consumers who have opted-out of the sale/sharing that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or collects from its own

interaction with consumers. A person who contracts with a business to provide cross-contextual behavioral advertising is a third party and not a service provider or contractor with respect to cross-contextual behavioral advertising services. Illustrative examples follow.

(1) Business S, a clothing company, hires a social media company as a service provider for the purpose of providing Business S's advertisements on the social media company's platform. The social media company can serve Business S by providing non-personalized advertising services on its platform based on aggregated or demographic information (e.g., advertisements to women, 18-30 years old, that live in Los Angeles). However, it cannot use a list of customer email addresses provided by Business S to identify users on the social media company's platform to serve advertisements to them.

(2) Business T, a company that sells cookware, hires an advertising company as a service provider for the purpose of advertising its services. The advertising agency can serve Business T by providing contextual advertising services, such as placing advertisements for Business T's products on websites that post recipes and other cooking tips.

~~(d) A service provider shall not sell data on behalf of a business when a consumer has opted out of the sale of their personal information with the business.~~

~~(c)~~ (e) If a service provider or contractor receives a request to know or a request to delete request made pursuant to the CCPA directly from the consumer, the service provider or contractor shall either act on behalf of the business in accordance with the business's instructions for responding to the request or inform the consumer that the request cannot be acted upon because the request has been sent to a service provider or contractor.

~~(d)~~ (f) A service provider or contractor that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider or contractor.

(e) A person who does not have a contract that complies with section 7051, subsection (a), is not a service provider or a contractor under the CCPA. For example, a business's disclosure of personal information to a person who does not have a contract that complies with section 7051, subsection (a) may be considered a sale or sharing of personal information for which the business must provide the consumer with the right to opt-out of sale/sharing.

(f) A service provider or a contractor shall comply with the terms of the contract required by the CCPA and these regulations.

(g) Whether an entity that provides services to a Nonbusiness must comply with a consumer's CCPA request depends upon whether the entity is a "business," as defined by Civil Code section 1798.140, subdivision (d).



*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.*

**§ 7051. Contract Requirements for Service Providers and Contractors.**

(a) The contract required by the CCPA for service providers and contractors shall:

- (1) Prohibit the service provider or contractor from selling or sharing personal information it Collects pursuant to the written contract with the business.
- (2) Identify the specific Business Purpose(s) for which the service provider or contractor is processing personal information pursuant to the written contract with the business, and specify that the business is disclosing the personal information to the service provider or contractor only for the limited and specified Business Purpose(s) set forth within the contract. The Business Purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
- (3) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any purpose other than the Business Purpose(s) specified in the contract or as otherwise permitted by the CCPA and these regulations.
- (4) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business for any commercial purpose other than the Business Purposes specified in the contract, unless expressly permitted by the CCPA or these regulations.
- (5) Prohibit the service provider or contractor from retaining, using, or disclosing the personal information that it Collected pursuant to the written contract with the business outside the direct business relationship between the service provider or contractor and the business, unless expressly permitted by the CCPA or these regulations. For example, a service provider or contractor shall be prohibited from combining or updating personal information that it Collected pursuant to the written contract with the business with personal information that it received from another source or Collected from its own interaction with the consumer, unless expressly permitted by the CCPA or these regulations.
- (6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it Collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

- (7) Grant the business the right to take reasonable and appropriate steps to ensure that the service provider or contractor uses the personal information that it Collected pursuant to the written contract with the business in a manner consistent with the business's obligations under the CCPA and these regulations. Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits, or other technical and operational testing at least once every 12 months.
- (8) Require the service provider or contractor to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
- (9) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate the service provider or contractor's unauthorized use of personal information. For example, the business may require the service provider or contractor to provide documentation that verifies that they no longer retain or use the personal information of consumers that have made a valid request to delete with the business.
- (10) Require the service provider or contractor to enable the business to comply with consumer requests made pursuant to the CCPA or require the business to inform the service provider or contractor of any consumer request made pursuant to the CCPA that they must comply with and provide the information necessary for the service provider or contractor to comply with the request.
- (b) A service provider or contractor that subcontracts with another person in providing services to the business for whom it is a service provider or contractor shall have a contract with the subcontractor that complies with the CCPA and these regulations, including subsection (a).
- (c) Whether a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

**§ 7052. Third Parties.**

- (a) A third party that does not have a contract that complies with section 7053, subsection (a), shall not collect, use, process, retain, sell, or share the personal information that the business made available to it.

(b) A third party shall comply with the terms of the contract required by the CCPA and these regulations, which include treating the personal information that the business made available to it in a manner consistent with the business's obligations under the CCPA and these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

**§ 7053. Contract Requirements for Third Parties.**

(a) A business that sells or shares a consumer's personal information with a third party shall enter into an agreement with the third party that:

- (1) Identifies the limited and specified purpose(s) for which the personal information is made available to the third party. The purpose shall not be described in generic terms, such as referencing the entire contract generally. The description shall be specific.
- (2) Specifies that the business is making the personal information available to the third party only for the limited and specified purposes set forth within the contract and requires the third party to use it only for those limited and specified purposes.
- (3) Requires the third party to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that the business makes available to the third party—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the third party to comply with a consumer's request to opt-out of sale/sharing forwarded to it by a first party business and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.
- (4) Grants the business the right—with respect to the personal information that the business makes available to the third party—to take reasonable and appropriate steps to ensure that the third party uses it in a manner consistent with the business's obligations under the CCPA and these regulations. For example, the business may require the third party to attest that it treats the personal information the business made available to it in the same manner that the business is obligated to treat it under the CCPA and these regulations.
- (5) Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information made available to the third party. For example, the business may require the third party to provide documentation that verifies that it no longer retains or uses the personal information of consumers who have had their requests to opt-out of sale/sharing forwarded to it by the first party business.

- (6) Requires the third party to notify the business after it makes a determination that it can no longer meet its obligations under the CCPA and these regulations.
- (b) Whether a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations. For example, depending on the circumstances, a business that never enforces the terms of the contract might not be able to rely on the defense that it did not have reason to believe that the third party intends to use the personal information in violation of the CCPA and these regulations at the time of the business disclosed the personal information to the third party.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.

## ARTICLE 5. VERIFICATION OF REQUESTS

### § 7060. General Rules Regarding Verification.

- (a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request ~~to know or a request to delete, request to correct, or request to know~~ is the consumer about whom the business has collected information.
- (b) A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license.
- (c) ~~(b)~~ In determining the method by which the business will verify the consumer's identity, the business shall:
- (1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.
  - (2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5, subdivision (d), unless necessary for the purpose of verifying the consumer.
  - (3) Consider the following factors:
    - (A) The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive ~~or valuable~~ personal information shall warrant a more stringent verification process. ~~The types of personal information identified in Civil Code section 1798.81.5, subdivision (d), shall be considered presumptively sensitive;~~

- (B) The risk of harm to the consumer posed by any unauthorized ~~access or deletion, correction, or access.~~ A greater risk of harm to the consumer by unauthorized ~~access or deletion, correction, or access~~ shall warrant a more stringent verification process.
  - (C) The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be.
  - (D) Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated.
  - (E) The manner in which the business interacts with the consumer, ~~and~~
  - (F) Available technology for verification.
- (d) ~~(e)~~ A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101.
- (e) ~~(d)~~ A business shall not require the consumer or the consumer's authorized agent to pay a fee for the verification of their request to ~~know or request to delete, request to correct, or request to know.~~ For example, a business may not require a consumer to provide a notarized affidavit to verify their identity unless the business compensates the consumer for the cost of notarization.
- (f) ~~(e)~~ A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized ~~access to or deletion, correction, or access~~ of a consumer's personal information.
- (g) ~~(f)~~ If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.
- (h) For requests to correct, the business shall make an effort to verify the consumer based on personal information that is not the subject of the request to correct. For example, if the consumer is contending that the business has the wrong address for the consumer, the business shall not use address as a means of verifying the consumer's identity.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135, 1798.140 and 1798.185, Civil Code.*

**§ 7061. Verification for Password-Protected Accounts.**

- (a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 7060. The business shall also require a consumer to re-authenticate themselves before ~~disclosing or deleting, correcting, or disclosing~~ the consumer's data.
- (b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete, request to correct, or request to know until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 7062 to further verify the identity of the consumer.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

**§ 7062. Verification for Non-Accountholders.**

- (a) If a consumer does not have or cannot access a password-protected account with a business, the business shall comply with this section, in addition to section 7060.
- (b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business that it has determined to be reliable for the purpose of verifying the consumer.
- (c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. If a business uses this method for verification, the business shall maintain all signed declarations as part of its record-keeping obligations.
- (d) A business's compliance with a request to delete or a request to correct may require that the business verify the identity of the consumer to a reasonable or reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion or correction. For example, the deletion of family photographs or the correction of contact information may require a reasonably high degree of certainty, while the deletion of browsing history or correction of marital status may require only a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with these regulations.

(e) Illustrative examples follow:

- (1) *Example 1:* If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if a retailer maintains a record of purchases made by a consumer, the business may require the consumer to identify items that they recently purchased from the store or the dollar amount of their most recent purchase to verify their identity to a reasonable degree of certainty.
- (2) *Example 2:* If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the personal information. For example, a business may have a mobile application that collects personal information about the consumer but does not require an account. The business may determine whether, based on the facts and considering the factors set forth in section 7060, subsection (b)(3), it may reasonably verify a consumer by asking them to provide information that only the person who used the mobile application may know or by requiring the consumer to respond to a notification sent to their device.

- (f) A business shall deny a request to know specific pieces of personal information if it cannot verify the identity of the requestor pursuant to these regulations.
- (g) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and explain why it has no reasonable method by which it can verify the identity of the requestor. If the business has no reasonable method by which it can verify any consumer, the business shall explain why it has no reasonable verification method in its privacy policy. The business shall evaluate and document whether a reasonable method can be established at least once every 12 months, in connection with the requirement to update the privacy policy set forth in Civil Code section 1798.130, subdivision (a)(5).

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

### **§ 7063. Authorized Agents.**

- (a) When a consumer uses an authorized agent to submit a request to know or a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request. The business may also require the consumer to do either of the following:
  - (1) Verify their own identity directly with the business.
  - (2) Directly confirm with the business that they provided the authorized agent permission to submit the request.
- (b) Subsection (a) does not apply when a consumer has provided the authorized agent with

power of attorney pursuant to Probate Code sections 4121 to 4130. A business shall not require power of attorney in order for a consumer to use an authorized agent to act on their behalf.

- (c) An authorized agent shall implement and maintain reasonable security procedures and practices to protect the consumer's information.
- (d) An authorized agent shall not use a consumer's personal information, or any information collected from or about the consumer, for any purposes other than to fulfill the consumer's requests, verification, or fraud prevention.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.130 and 1798.185, Civil Code.*

## **ARTICLE 6. SPECIAL RULES REGARDING CONSUMERS UNDER 16 YEARS OF AGE**

### **§ 7070. Consumers Less Than Under-13 Years of Age.**

#### **(a) Process for Opting-In to Sale or Sharing of Personal Information**

- (1) A business that has actual knowledge that it sells or shares the personal information of a consumer less than under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person ~~affirmatively authorizing~~ consenting to the sale or sharing of the personal information about the child is the parent or guardian of that child. ~~This affirmative authorization consent to the sale or sharing of personal information is in addition to any verifiable parental consent required under COPPA.~~
- (2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include, but are not limited to:
  - (A) Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;
  - (B) Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
  - (C) Having a parent or guardian call a toll-free telephone number staffed by trained personnel;
  - (D) Having a parent or guardian connect to trained personnel via video-conference;
  - (E) Having a parent or guardian communicate in person with trained personnel; and
  - (F) Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, as long as the parent



or guardian's identification is deleted by the business from its records promptly after such verification is complete.

- (b) When a business receives ~~an affirmative authorization consent~~ to the sale or sharing of personal information pursuant to subsection (a), the business shall inform the parent or guardian of the right to opt-out of sale/sharing and of the process for doing so on behalf of their child pursuant to section 7026, subsections (a)-(f).
- (c) A business shall establish, document, and comply with a reasonable method, in accordance with the methods set forth in subsection (a)(2), for determining that a person submitting a request to ~~know or a request to delete,~~ request to correct, or request to know the personal information of a child under the age of 13 is the parent or guardian of that child.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

**§ 7071. Consumers at Least 13 Years of Age and Less Than 16 to 15 Years of Age.**

- (a) A business that has actual knowledge that it sells or shares the personal information of consumers at least 13 years of age and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such consumers to opt-in to the sale or sharing of their personal information, pursuant to section 7028.
- (b) When a business receives a request to opt-in to the sale or sharing of personal information from a consumer at least 13 years of age and less than 16 years of age, the business shall inform the consumer of their ongoing right to opt-out of sale/sharing at any point in the future a later date and of the process for doing so pursuant to section 7026.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

**§ 7072. Notices to Consumers Less Than Under 16 Years of Age.**

- (a) A business subject to sections 7070 and/or 7071 shall include a description of the processes set forth in those sections in its privacy policy.
- (b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell or share the personal information without the ~~affirmative authorization consent~~ of consumers at least 13 years of age and less than 16 years of age, or the ~~affirmative authorization consent~~ of their parent or guardian for consumers under 13 years of age, is not required to provide the ~~Notice of Right to Opt-out of Sale/Sharing.~~

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.*

## ARTICLE 7. NON-DISCRIMINATION

### § 7080. Discriminatory Practices.

- (a) A ~~financial incentive or a price~~ or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.
- (b) A business may offer a ~~financial incentive or price~~ or service difference that is non-discriminatory. A price or service difference is non-discriminatory if it is reasonably related to the value of the consumer's data. If a business is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the ~~financial incentive or price~~ or service difference is reasonably related to the value of the consumer's data, that business shall not offer the ~~financial incentive or price~~ or service difference.
- (c) A business's denial of a consumer's request to ~~know, request to delete, request to correct,~~ request to know, or request to opt-out of sale/sharing for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.
- (d) Illustrative examples follow:
  - (1) *Example 1:* A music streaming business offers a free service as well as a premium service that costs \$5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale or sharing of their personal information, then the practice is discriminatory, unless the \$5-per-month payment is reasonably related to the value of the consumer's data to the business.
  - (2) *Example 2:* A clothing business offers a loyalty program whereby customers receive a \$5-off coupon by email after spending \$100 with the business. A consumer submits a request to delete all personal information the business has collected about them but also informs the business that they want to continue to participate in the loyalty program. The business may deny their request to delete with regard to their email address and the amount the consumer has spent with the business because that information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with them pursuant to Civil Code section 1798.105, subdivision (d)(1).
  - (3) *Example 3:* A grocery store offers a loyalty program whereby consumers receive coupons and special discounts when they provide their phone numbers. A consumer submits a request to opt-out of the sale/sharing of their personal information. The retailer complies with their request but no longer allows the consumer to participate in the loyalty program. This practice is discriminatory unless the grocery store can demonstrate that the value of the coupons and special discounts are reasonably related to the value of the consumer's data to the business.
  - (4) *Example 4:* An online bookseller collects information about consumers, including their email addresses. It offers coupons to consumers through browser pop-up

windows while the consumer uses the bookseller's website. A consumer submits a request to delete all personal information that the bookseller has collected about them, including their email address and their browsing and purchasing history. The bookseller complies with the request but stops providing the periodic coupons to the consumer. The bookseller's failure to provide coupons is discriminatory unless the value of the coupons is reasonably related to the value provided to the business by the consumer's data. The bookseller may not deny the consumer's request to delete with regard to the email address because the email address is not necessary to provide the coupons or reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

- (e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 7016.
- (f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145, subdivision (h)(3), shall not be considered a financial incentive subject to these regulations.
- (g) A price or service difference that is the direct result of compliance with a state or federal law shall not be considered discriminatory.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.*

#### **§ 7081. Calculating the Value of Consumer Data**

- (a) A business offering a ~~financial incentive or price~~ or service difference subject to Civil Code section 1798.125 shall use and document a reasonable and good faith method for calculating the value of the consumer's data. The business shall consider one or more of the following:
  - (1) The marginal value to the business of the sale, collection, or deletion of a consumer's data.
  - (2) The average value to the business of the sale, collection, or deletion of a consumer's data.
  - (3) The aggregate value to the business of the sale, collection, or deletion of consumers' data divided by the total number of consumers.
  - (4) Revenue generated by the business from sale, collection, or retention of consumers' personal information.
  - (5) Expenses related to the sale, collection, or retention of consumers' personal information.
  - (6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference.

- (7) Profit generated by the business from sale, collection, or retention of consumers' personal information.
  - (8) Any other practical and reasonably reliable method of calculation used in good faith.
- (b) For the purpose of calculating the value of consumer data, a business may consider the value to the business of the data of all natural persons in the United States and not just consumers.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130 and 1798.185, Civil Code.*

## **ARTICLE 8. TRAINING, AND RECORD-KEEPING**

### **§ 7100. Training.**

- (a) All individuals responsible for handling consumer inquiries about the business's ~~privacy information p~~ practices or the business's compliance with the CCPA shall be informed of all of the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.
- (b) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests made under the CCPA or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.125, 1798.130, 1798.135 and 1798.185, Civil Code.*

### **§ 7101. Record-Keeping.**

- (a) A business shall maintain records of consumer requests made pursuant to the CCPA and how it responded to the requests for at least 24 months. The business shall implement and maintain reasonable security procedures and practices in maintaining these records.
- (b) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.
- (c) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

- (d) Information maintained for record-keeping purposes shall not be used for any other purpose except as reasonably necessary for the business to review and modify its processes for compliance with the CCPA and these regulations. Information maintained for record-keeping purposes shall not be shared with any third party except as necessary to comply with a legal obligation.
- (e) Other than as required by subsection (b), a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100~~, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.*

**§ 7102. Requirements for Businesses Collecting Large Amounts of Personal Information.**

- (a) A business that knows or reasonably should know that it, alone or in combination, buys, receives for the business's commercial purposes, sells, ~~or shares,~~ or otherwise makes available for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year shall:
  - (1) Compile the following metrics for the previous calendar year:
    - (A) ~~The number of requests to know that the business received, complied with in whole or in part, and denied;~~ (B) ~~The number of requests to delete that the business received, complied with in whole or in part, and denied;~~
    - (B) The number of requests to correct that the business received, complied with in whole or in part, and denied;
    - (C) The number of requests to know that the business received, complied with in whole or in part, and denied;
    - (D) ~~(C)~~ The number of requests to opt-out of sale/sharing that the business received, complied with in whole or in part, and denied; ~~and~~
    - (E) The number of requests to limit that the business received, complied with in whole or in part, and denied; and
    - (F) ~~(D)~~ The median or mean number of days within which the business substantively responded to ~~requests to know,~~ requests to delete, requests to correct, requests to know, requests to opt-out of sale/sharing, and requests to ~~opt-out limit.~~
  - (2) Disclose, by July 1 of every calendar year, the information compiled in subsection (a)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy. ~~(A)~~ In its disclosure pursuant to subsection (a)(2), a business may choose to disclose the number of requests that it denied in whole or in

part because the request was not verifiable, was not made by a consumer, called for information exempt from disclosure, or was denied on other grounds.

- (b) A business may choose to compile and disclose the information required by subsection (a)(1) for requests received from all individuals, rather than requests received from consumers. The business shall state whether it has done so in its disclosure and shall, upon request, compile and provide to the Attorney General the information required by subsection (a)(1) for requests received from consumers.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections ~~1798.100~~, 1798.105, 1798.106, 1798.110, 1798.115, 1798.120, 1798.121, 1798.130, 1798.135 and 1798.185, Civil Code.*

## **ARTICLE 9. INVESTIGATIONS AND ENFORCEMENT**

### **§ 7300. Sworn Complaints Filed with the Agency.**

- (a) Requirements for filing a sworn complaint. Sworn complaints may be filed with the Enforcement Division via the electronic complaint system available on the Agency's website at <https://cppa.ca.gov/> or submitted in person or by mail to the headquarters office of the Agency.

A complaint must:

- (1) Identify the business, service provider, contractor, or person who allegedly violated the CCPA;
  - (2) State the facts that support each alleged violation and include any documents or other evidence supporting this conclusion;
  - (3) Authorize the alleged violator and Agency to communicate regarding the complaint, including disclosing the complaint and any information relating to the complaint;
  - (4) Include the name and current contact information of the complainant; and
  - (5) Be signed and submitted under penalty of perjury.
- (b) The Enforcement Division will notify the complainant in writing of the action, if any, the Agency has taken or plans to take on the complaint, together with the reasons for that action or nonaction. Duplicate complaints submitted by the same complainant may be rejected without notice.

*Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.*

**§ 7301. Investigations.**

- (a) The Agency may initiate investigations from referrals from government agencies or private organizations, and sworn, nonsworn, or anonymous complaints, or on the Agency's own initiative.
- (b) As part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.45, Civil Code.

**§ 7302. Probable Cause Proceedings.**

- (a) Probable Cause. Under Civil Code section 1798.199.50, probable cause exists when the evidence supports a reasonable belief that the CCPA has been violated.
- (b) Probable Cause Notice. The Enforcement Division will provide the alleged violator with notice of the probable cause proceeding as required by Civil Code section 1798.199.50.
- (c) Probable Cause Proceeding.
  - (1) The proceeding shall be closed to the public unless the alleged violator files, at least 10 business days before the proceeding, a written request for a public proceeding. If the proceeding is not open to the public, then the proceeding may be conducted in whole or in part by telephone or videoconference.
  - (2) The Agency shall conduct the proceeding informally. Only the alleged violator(s), their legal counsel, and Enforcement Division shall have the right to participate at the proceeding. The Agency shall determine whether there is probable cause based on the probable cause notice and any information or arguments presented at the probable cause proceeding by the parties.
  - (3) If the alleged violator(s) fails to participate or appear at the probable cause proceeding, the alleged violator(s) waives the right to further probable cause proceedings under Civil Code section 1798.199.50, and the Agency shall determine whether there is probable cause based on the notice and any information or argument provided by the Enforcement Division.
- (d) Probable Cause Determination. The Agency shall issue a written decision with its probable cause determination and serve it on the alleged violator electronically or by mail. The Agency's probable cause determination is final and not subject to appeal.

- (e) Notices of probable cause and probable cause determinations shall not be open to the public nor admissible in evidence in any action or special proceeding other than one enforcing the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.199.50, Civil Code.

**§ 7303. Stipulated Orders.**

- (a) At any time before or during an administrative hearing and in lieu of such a hearing, the Head of Enforcement and the alleged violator may stipulate to the entry of a final order. If a stipulation has been agreed upon and the scheduled date of the hearing is set to occur before the next Board meeting, the Enforcement Division will apply for a continuance of the hearing.
- (b) The final order must be approved by the Board, which may consider the matter in closed session.
- (c) The stipulated final order shall be public and have the force of an order of the Board.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.199.35 and 1798.199.55, Civil Code.

**§ 7304. Agency Audits.**

- (a) Scope. The Agency may audit a business, service provider, contractor, or person to ensure compliance with any provision of the CCPA.
- (b) Criteria for Selection. The Agency may conduct an audit to investigate possible violations of the CCPA. Alternatively, the Agency may conduct an audit if the subject's collection or processing of personal information presents significant risk to consumer privacy or security, or if the subject has a history of noncompliance with the CCPA or any other privacy protection law.
- (c) Audits may be announced or unannounced as determined by the Agency.
- (d) Failure to Cooperate. A subject's failure to cooperate during the Agency's audit may result in the Agency issuing a subpoena, seeking a warrant, or otherwise exercising its powers to ensure compliance with the CCPA.
- (e) Protection of Personal Information. Consumer personal information disclosed to the Agency during an audit shall be maintained in compliance with the Information Practices Act of 1977, Civil Code section 1798, et seq.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.185, 1798.199.40 and 1798.199.65, Civil Code; Section 11180, Government Code.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

*Exhibit 5*

**FSOR APPENDIX A: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING 45-DAY PERIOD**

Response #	Summary of Comment	Response	Comment #s	Bates Label / Transcript CPPA_RMI_45D AY
<b>ARTICLE 1. GENERAL PROVISIONS</b>				
<b>§ 7001. Definitions</b>				
- <b>Comments about definitions not included</b>				
1.	Comment suggests adding a definition for "Alternative Opt-Out Link" and capitalizing the term throughout the regulations.	Accept. The proposed regulation has been modified to include a definition for "Alternative Opt-Out Link." See § 7001(b). This term has also been capitalized throughout the regulations.	W90-15	0983
2.	Comment suggests clarifying the meaning of third parties, as it remains undefined compared to the term "service providers."	No change has been made in response to this comment. Civ. Code § 1798.140(ai) defines the term "third party."	W11-41 W11-47	0151 0152
3.	Comment suggests that hashed personal information should still be treated as personal information. Businesses and service providers should not be able to avoid responding to CCPA requests because they only store hash values of personal information.	No change has been made in response to this comment. The statutory definition of "personal information" and includes any information that is reasonably capable of being associated with a particular consumer or household." See Civ. Code § 1798.140(v). Hashed information may be "personal information," but this is ultimately a fact-specific and contextual determination. Similarly, whether a business is required to respond to a request to know with hashed personal information is a fact-specific and contextual determination. See Civ. Code § 1798.145(j).	W19-1 W19-4 W19-5	0197-0198 0198 0198
4.	Comment recommends defining the term "precise geolocation" with specificity. Comment suggests adopting the same definition as the Network Advertising Initiative: "Precise geolocation" means identifying a consumer with more precision than longitude and latitude with two decimal places, or within the area of a circle with a radius of less than 500 meters with an accuracy of 68% or more.	No change has been made in response to this comment. The term "precise geolocation" is defined in Civ. Code § 1798.140(w). Further analysis is required to determine whether a regulation on this issue is necessary.	W102-1	1079
5.	Comments suggest defining the term "explicit consent" because §§ 7002(a), 7002(b)(1)-(b)(4) repeatedly use it and it should be defined to differ from "consent."	No change has been made in response to this comment. The Agency has modified the regulation and removed "explicit" in § 7002, and thus, this comment is now moot. In addition, "consent" is defined in the Civ. Code § 1798.140(h).	W20-13 W97-1	0208 1059-1060

**FSOR APPENDIX A: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING 45-DAY PERIOD**

Response #	Summary of Comment	Response	Comment #s	Bates Label / Transcript CPPA_RM1_45D AY
	undermine, technology industry efforts to provide baseline for data privacy practices that will continue to allow tech companies to flourish. Another comment contends that regulations will burden research and development in the fields of biotechnology, pharmaceuticals, and medical device technology, particularly small start-ups focused on discovering new medical breakthroughs, which often have few employees and limited funding.		O19-3 O24-1	D1 60:21-61:6 D2 14:2-14:24 15:3-15:11
703.	Comments disagree with businesses that argue that the regulations are confusing or burdensome. Comment states that the issue here is not technical capability and that aside from a general concern of burden, those commenters did not identify tangible obstacles or solutions to a middle ground. Comments state that businesses can make a simple decision to minimize data collection or not sell personal information for invasive and privacy-violating, cross-contextual advertising.	No change has been made in response to this comment. The comment appears to concur with the proposed regulations, so no further response is required.	O18-4 O30-1	D1 58:15-58:20 D2 34:1-34:22
- Delay				
704.	Comments suggest delaying the effective date and/or enforcement of the regulations for 6 to 18 months. Comments note that regulations implementing certain CCPA provisions remain forthcoming and that requiring businesses to comply before January 2024 will lead to confusion. Some comments suggest that businesses need	No change has been made in response to these comments. The Agency has made every effort to issue final regulations in a timely manner that comply with the CCPA and the rulemaking procedures. The Agency has considered delaying the effective date and/or the enforcement date of the regulations and has determined that doing so is not more effective in carrying out the purpose and intent of the CCPA than having the regulations take effect in accordance with the standard rules governing rulemaking. See Gov. Code	W11-54 W14-15 W52-33 W52-63 W69-57 W75-4 W89-50	0153-54 0167 0536 0553 0776 0815 0967

**FSOR APPENDIX A: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING 45-DAY PERIOD**

Response #	Summary of Comment	Response	Comment #s	Bates Label / Transcript CPPA_RM1_45D AY
	<p>more time to comply. Another comment recommends effectively delaying the enforcement or the proposed regulations to the employment and business-to-business contexts until the Agency engages in a separate rulemaking that the commenter recommends. Another comment also recommends delaying enforcement of the rules as applied to employment records, because businesses need time to apply the rulemaking to employment records and carry out required implementation, particularly because certain rights are incompatible with business functions and other legal obligations.</p>	<p>§ 11343.4(a). The proposed regulations provide comprehensive guidance to consumers, businesses, service providers, and third parties on how to implement and operationalize new consumer privacy rights and other changes to the law introduced by the CPRA amendments to the CCPA. The Agency has determined that delaying the regulations will cause greater confusion for consumers and businesses. In addition, the Agency has determined that businesses will have sufficient time to comply with the regulations before the Agency's enforcement commences. Although the proposed regulations are not yet final and have been subject to public comment and amendments, businesses have been aware of the proposed regulations' general contours since July 8, 2022, when they were released. Many of these regulations have been in effect with only slight modifications since 2020. Moreover, when considering whether to investigate a violation or initiate an enforcement action, the Agency, in the exercise of its prosecutorial discretion, may consider the effect that the delay in adopting the regulations has had on a business's ability to comply. Prosecutorial discretion permits the Agency to choose which entities to investigate and whether to initiate an administrative action. How the Agency decides to exercise its enforcement authority is a context-specific, fact-specific, discretionary decision. Proposed regulation § 7301(b) recognizes that, when the Agency investigates violations of the CCPA or its implementing regulations, the Agency has the discretionary authority to consider the effective date of statutory and regulatory requirements and businesses' good-faith efforts to comply with the law.</p>		
705.	<p>Comments suggest delaying the effective date of the regulations or delaying enforcement of the regulations. Comments suggest that the purpose of the July 1, 2022 statutory date for regulations in Civil Code</p>	<p>No change has been made in response to these comments. The Agency has made every effort to issue final regulations in a timely manner that comply with the CCPA and the rulemaking procedures. The Agency has considered delaying the effective date and/or the enforcement date of the regulations and has determined that doing</p>	<p>W28-1 W29-13 W33-21 W35-2 W37-33</p>	<p>0274 0326-0327 0362 0371 0397</p>

**FSOR APPENDIX A: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING 45-DAY PERIOD**

Response #	Summary of Comment	Response	Comment #s	Bates Label / Transcript CPPA_RM1_45D AY
	<p>§ 1798.185(d) was to provide businesses with six months or more to comply with the regulations. Comments suggest that businesses must have fair and reasonable notice to comply and that they will need a period of time to implement the regulations, to revise policies and procedures, to make changes to digital properties, etc. Comments request guidance on when the proposed regulations will come into effect and when the Agency will commence enforcement. Comment suggests delaying the regulations until an independent economic study can determine the impact of the loss of ad revenue and final regulations can minimize that impact. Comments also request that the Agency take into account the impact the regulations and missed deadlines will have on businesses and innovation, and the difficulty for small businesses in understanding and complying with the complex regulatory framework.</p>	<p>so is not more effective in carrying out the purpose and intent of the CCPA than having the regulations take effect in accordance with the standard rules governing rulemaking. See Gov. Code § 11343.4(a). Although Civil Code § 1798.185(d) directed the Agency to adopt final regulations required by the Act by July 1, 2022, that directive must be read in conjunction with the CCPA's overarching purpose and intent. The voters intended the law to take effect on January 1, 2023, and for enforcement to begin July 1, 2023. Delaying the regulations or enforcement would deprive millions of California consumers of the rights codified in the CCPA. Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3(A); Civ. Code §§ 1798.105-125. In addition, the Agency has determined that businesses will have sufficient time to comply with the regulations before the Agency's enforcement commences. Although the proposed regulations are not yet final and have been subject to public comment and amendments, businesses have been aware of the proposed regulations' general contours since July 8, 2022, when they were released. Many of these regulations have been in effect with only slight modifications since 2020. Moreover, when considering whether to investigate a violation or initiate an enforcement action, the Agency, in the exercise of its prosecutorial discretion, may consider the effect that the delay in adopting the regulations has had on a business's ability to comply. Prosecutorial discretion permits the Agency to choose which entities to investigate and whether to initiate an administrative action. How the Agency decides to exercise its enforcement authority is a context-specific, fact-specific, discretionary decision. Proposed regulation § 7301(b) recognizes that, when the Agency investigates violations of the CCPA or its implementing regulations, the Agency has the discretionary authority to consider the effective date of statutory and regulatory requirements and businesses' good-faith efforts to comply with the law. With regard to when the regulations</p>	<p>W41-1 W43-27 W44-2 W44-3 W45-1 W52-34 W53-3 W54-2 W59-72 W61-2 W72-1 W75-32 W76-1 W80-12 W80-13 W84-23 W89-3 W89-4 O2-3 O4-1 O5-1 O8-1 O10-1 O13-1 O14-1 O17-3 O19-1 O20-1</p>	<p>0421 0443 0449 0449 0467 0536-0537 0561 0571 0618 0649 0798 0832 0835 0877 0877 0924 0951 0951 D1 14:14-14:18 D1 16:6-16:21 D1 17:21-18:14 D1 27:17-27:21 D1 33:13-33:22 D1 43:9-43:19 D1 45:22-47:19 D1 56:17-56:25 D1 59:12-60:3 D1 62:10-63:8</p>

**FSOR APPENDIX A: SUMMARY AND RESPONSE TO COMMENTS SUBMITTED DURING 45-DAY PERIOD**

Response #	Summary of Comment	Response	Comment #s	Bates Label / Transcript CPPA_RM1_45D AY
		<p>will come into effect, that process is governed by statute and administered by the Office of Administrative Law. The Agency encourages those interested in the regulatory process to join the Agency's email listserv to receive updates on the rulemaking process. Lastly, the Agency complied with the Administrative Procedure Act's requirements for its economic analysis, which contemplates the cost of complying with the regulations, not the baseline costs associated with complying with existing law or regulations. The impact on the availability of cross-contextual advertising is a result of the statute, not the regulations, and is not a basis to delay the regulations.</p>		
706.	<p>Comments suggest that the agency engage in a longer deliberative process to account for potential developments in federal privacy statutes and regulations or the privacy laws and regulations of other states.</p>	<p>No change has been made in response to these comments. The Agency has considered delaying the enforcement of the regulations and has determined that doing so is not more effective in carrying out the purpose and intent of the CCPA than having the regulations take effect in accordance with the standard rules governing rulemaking. See Gov. Code § 11343.4(a). Waiting for laws or regulations that may or may not be enacted in other jurisdictions would not advance consumer privacy or promote business compliance.</p>	W34-1 W89-4	0366 0951
707.	<p>Comments suggest delaying enforcement with regard to automated decision-making, privacy risk assessments, and cybersecurity audits.</p>	<p>No change has been made because the comments are not directed at any proposed regulation, or the rulemaking procedures followed. The Agency has not addressed automated decision-making technology, privacy risk assessments, or cybersecurity audits at this time. The Agency has prioritized the drafting of regulations that operationalize and assist in the immediate implementation of the law. These other topics will be the subject of future rulemaking.</p>	W37-33 W65-22	0397 0721
708.	<p>Comment suggests that Agency "work with the Legislature" to extend the July 1, 2022 statutory deadline for finalizing regulations and July 1, 2023 statutory date on which enforcement actions may commence, such</p>	<p>No change has been made in response to this comment. The comment proposes legislative action and is therefore not directed at the proposed regulations, or the rulemaking procedures followed.</p>	W54-1 O1-2 O1-5 O12-1	0569-70 D1 11:4-11:12 D1 12:4-12:12 D1 41:8-42:13