Morgan Lewis

CALIFORNIA CONSUMER PRIVACY ACT CHECKLIST

1. Determine whether the California Consumer Privacy Act (CCPA) applies to your business.

- **A business is only subject to the CCPA if it**
  - Is for profit,
  - Does business in California,
  - Collects consumers' personal information, and
  - Determines the purposes and means of processing consumers' personal information.
- **In addition, the CCPA only applies to a business that**
  - Has annual gross revenue in excess of $25 million;
  - Annually buys, receives for commercial purposes, sells, or shares for commercial purposes personal information of 50,000 or more consumers, households, or devices; or
  - Derives 50% or more of its annual revenue from selling consumers' personal information.
- **Exceptions: The CCPA does not apply to**
  - Medical information collected by a covered entity governed by the Health Insurance Portability and Accountability Act (HIPAA) or California Confidentiality of Medical Information Act (CMIA); entities subject to HIPAA or CMIA; or information collected as part of a clinical trial;
  - Personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act or
  - California Financial Privacy Information Act;
  - Information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994;
  - The sale of personal information to or from a consumer reporting agency to be reported in or used to generate a consumer report;
  - Efforts to comply with federal, state, or local law; a civil, criminal, or regulatory investigation; or a subpoena or summons;
  - Cooperation with law enforcement agencies or exercising/defending legal claims;
  - Until January 1, 2021: Personal information collected from job applicants, employees, owners, directors, staff, officers and contractors of a business (except that employees will be subject to the "notice at collection" requirements, which must describe the categories of personal information collected and the purposes for which personal information will be used.);
  - Until January 1, 2021: Personal information about an employee, owner, director, officer or contractor collected pursuant to due diligence or a business-to- business communication or transaction; or
  - Vehicle information and vehicle ownership information retained or shared by dealers and vehicle manufacturers for warranty or recall-related repair.

2. Determine what data elements are collected from California consumers and for what purposes they are used.

- The scope of "personal information" under the CCPA is broad and includes any 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," including the following 11 enumerated categories of consumer information:

1. Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, and passport number.
2. Personal information under California's records destruction law (Cal. Civ. Code § 1798.80(e)), which additionally includes signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, or financial account information.
3. Characteristics of protected classifications under California or federal law.
4. Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
5. Biometric information.
6. Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement.
7. Geolocation data.
8. Audio, electronic, visual, thermal, olfactory, or similar information.
9. Professional or employment-related information.
10. Education information that is not publicly available personally identifiable information, as defined in the Family Educational Rights and Privacy Act (20 USC § 1232(g), 34 CFR Part 99).
11. Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

- Excluded from this definition is "aggregate consumer information," which is defined as data that is "not linked or reasonably linkable to any consumer or household, including via a device," as well as information that is publicly available from federal, state, or local government records.

3. Consider how consumers' personal information should be organized.

- Provide required CCPA notices and opt-out and opt-in rights (see steps 4, 5, 10).
- Delete data to comply with the CCPA's right to delete (see steps 5, 7(B), 8).
- Provide consumer data upon request in a "readily useable format" (see step 6).
- Ensure that agreements with service providers are CCPA compliant (see step 12).
- Train personnel to properly process new requests to exercise privacy rights (see step 11).

4. Revise your website's home page.

- **Right to opt out of sale of personal information to third parties**. If a business sells personal information, the business must provide notice to consumers that their personal information may be sold and inform consumers that they have the right to opt out of such sale. In order to comply with this right to opt out, a business must post a "clear and conspicuous link" on its website's home page titled "Do Not Sell My Personal Information," and describe the right in its privacy policy (see step 5). If a business collects personal information through a mobile application, it may provide a link to the notice and opt out requirements on the application's download page and settings menu.

5. Revise your privacy policy.

- Businesses covered by the CCPA must provide, at or before the point of collection, in their website privacy policy or otherwise, a privacy policy that includes the following:
- **Right to know**.
  - The categories of personal information to be collected about the consumer and the purposes for which the information will be used,
  - The categories of sources from which personal information is collected, and
  - The categories of consumers' personal information that were actually collected in the preceding 12 months and sold or disclosed for business purposes in the preceding 12 months.
- **Right to delete**. Businesses must also inform consumers of their right to request deletion of their personal information.
- **Right to opt out of sale of personal information to third parties**. In order to comply with the right to opt out, a business must describe the right in its privacy policy. A business must either state that it does not sell personal information or describe how the opt-out right may be exercised.

6. Create a process for submitting requests to know and to delete and identify individuals responsible for responding to "verifiable consumer requests."

- Businesses must make available two or more designated methods for the consumer to request this information, including, at a minimum, a toll-free telephone number.

- However, a business that operates exclusively online and has a direct relationship with a consumer is only required to provide an email address for submitting requests.
- Consumers have the right to make such requests twice in any 12-month period.

7. Create a process to timely confirm requests to know and requests to delete, and to verify requestors.

- Businesses must confirm receipt of a request to know or delete within 10 business days and provide information about their processing of the requests, including a description of businesses' verification process.
- Businesses must respond to a request to know or delete within 45 calendar days, by mail or electronically.
- If a business cannot verify identity of the consumer making a request to know or delete, it may deny the request and must inform the requestor that its identity cannot be verified.

(A) Responding to requests to know: Create a process and identify individuals responsible for preserving copies of "specific pieces of personal information that the business has collected about [each] consumer" and promptly responding to consumers' requests to access same.

- Information provided pursuant to a request to know must be portable, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity "without hindrance."
- There is an exception for personal information that is collected for "single, one-time transactions."
- In response to such requests, the CCPA requires businesses to disclose:
  - The categories of personal information the business collected about the consumer,
  - The categories of sources from which personal information is collected,
  - The business or commercial purpose for collecting or selling personal information,
  - The categories of third parties with whom the business shares personal information,
  - The specific pieces of personal information the business has collected about the consumer, and
  - The categories of the consumer's personal information that were sold or disclosed for business purposes in the 12 months preceding the consumer's verifiable request.

(B) Responding to requests to delete: Create a process and identify individuals responsible for deleting consumer data in response to such a request.

- Exceptions to requests to delete include where retention of the consumer's personal information is necessary to:
  - Complete a transaction for which the personal information was collected, provide goods and services to the consumer, or otherwise perform a contract with the consumer;
  - Detect security incidents, fraud, or illegal activity;
  - Exercise free speech, or ensure the right of another consumer to exercise his or her right of free speech;
  - Enable internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
  - Comply with a legal obligation; or
  - Otherwise use the consumer's personal information internally and in a lawful manner that is compatible with the context in which the consumer provided the information.

8. Create policies that reconcile the CCPA's requirement to delete data upon request with the need to preserve evidence in litigation and avoid sanctions for spoliation of evidence.

9. Create a process to timely comply with a request to opt-out of sale.

- The request need not be a verifiable request.
- Businesses must comply with a request to opt out of sale no later than 15 business days and direct third parties not to sell the consumer's information.

10. Provide consumers under 16 years of age with a "right to opt in."

- Businesses are prohibited from selling personal information of consumers between the ages of 13 and 15 without first obtaining affirmative opt-in consent (1) from the consumer or (2) from a parent or guardian where the consumer is under the age of 13.

11. Provide training for employees on the CCPA's prescribed consumer rights.

- Businesses must ensure that personnel responsible for handling consumer inquiries regarding these new privacy rights are informed of the applicable requirements of the CCPA and CCPA regulations, and know how to direct consumers to exercise those rights.

12. Review existing agreements with third parties or service providers to ensure that contracts limit the service provider's use of personal information as strictly as the CCPA prescribes, and revise as needed.

- The CCPA allows businesses to share personal information with third parties or service providers for business purposes, so long as there is a written contract prohibiting the third party or service provider from selling the personal information or "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."
- The CCPA defines "business purpose" as "the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected." The CCPA enumerates categories of activities that constitute "business purposes," including auditing; detecting security incidents; performing services, such as maintaining or servicing accounts, providing customer service, processing payments, fulfilling orders and transactions, and providing analytic services; and undertaking internal research for technological development and demonstration.
- Without a CCPA-compliant service provider agreement, the disclosure of personal information to a vendor may constitute a sale of personal information that triggers the consumer's opt-out right.

13. Provide consumers the right to equal service and price.

- Prohibits businesses from discriminating against consumers who exercise their rights under the CCPA or CCPA regulations.
- A business is specifically prohibited from
  - Denying goods or services to a consumer,
  - Charging a consumer a different price or rate for goods or services, including through the use of discounts or other benefits,
  - Imposing penalties on a consumer,
  - Providing a consumer with a different level of quality of goods or services, and
  - Suggesting a consumer will receive a different price or rate or different level of quality of goods or services.

14. Create and maintain a robust incident response plan.

- While implementing a robust incident response plan has been a best practice for some time, the availability of statutory damages under the CCPA's private right of action for security breaches further underscores the need for a thoughtful and comprehensive approach to breach response because the act will almost certainly lead to a spike in data breach–related litigation in California.

Morgan Lewis

HOW WE CAN HELP

If we can be of assistance regarding the California Consumer Privacy Act, please contact a Morgan Lewis lawyer listed below:

W. Reece Hirsch
+1.415.442.1422
reece.hirsch@morganlewis.com

Mark L. Krotoski
+1.650.843.7212
mark.krotoski@morganlewis.com

Carla B. Oakley
+1.415.442.1301
carla.oakley@morganlewis.com

Tess Blair
+1.215.963.5161
tess.blair@morganlewis.com

Joseph Duffy
+1.213.612.7378
joseph.duffy@morganlewis.com

J. Warren Rissier
+1.213.680.6860
warren.rissier@morganlewis.com

Gregory T. Parks
+1.215.963.5170
gregory.parks@morganlewis.com

Ezra D. Church
+1.215.963.5710
ezra.church@morganlewis.com

Michelle Park Chiu
+1.415.442.1184
michelle.chiu@morganlewis.com

Kristin M. Hadgis
+1.215.963.5563
kristin.hadgis@morganlewis.com

Bryan P. Goff
+1.212.309.6157
bryan.goff@morganlewis.com

Terese Schireson
+1.215.963.4830
terese.schireson@morganlewis.com

Lauren Groebe
+1.312.324.1478
lauren.groebe@morganlewis.com

Melis S. Kiziltay Carter
+1.212.309.6194
melis.kiziltaycarter@morganlewis.com

www.morganlewis.com

090920_201813