ALERT

Countdown to CCPA: Do You Know Where Your Data Is?

Starting in 2020, "inventory management" takes on new meaning in California.

By Catherine D. Meyer and Fusae Nara

05.01.2019

TAKEAWAYS

- *Going into effect Jan. 1, 2020, the CCPA grants five new rights to consumers respecting personal information.*
- *Building a data inventory that includes the types of information that will be required for CCPA disclosures is a rational first step towards compliance.*

It's January 2, 2020, and you just received 25 requests asking for disclosure about your data collection, use and sharing practices and for a copy of the specific pieces of personal information you collected about the requesting individuals during the last 12 months. You have 45 days to respond. What do you do? Close down the business so you can find the information? By being prepared you can avoid a crisis.

The California Consumer Privacy Act of 2018 (CCPA) goes into effect on January 1, 2020, and affects for-profit companies selling goods or services in or into California with $25 Million in annual gross revenues or that meet thresholds for collection or sale of personal data on anyone residing in California. The Act grants "consumers" (any California resident regardless of whether there is a customer or any other relationship with the covered business) five new rights respecting their personal information:

1. The right to know your business' data collection practices including the categories of personal information you have collected, the source of the information, your use of the information and to whom you disclosed the information you have collected about them,
2. The right to receive a copy of the specific personal information collected about them during the 12 months before their request,
3. The right to have such information deleted (with exceptions),
4. The right to know your business' data sale practices and to request that their personal information not be sold to third parties, and
5. The right not to be discriminated against because they exercised a new right.

From the perspective of covered businesses, these new rights create obligations to expand and annually update their privacy policy disclosures, to provide the on-demand disclosures to verified consumers within 45 days of receiving a request, to delete personal information upon request, and to refrain from selling personal information upon request.[1]

The disclosures that the business will be required to make in its privacy policy and to on-demand requesting parties include the categories of personal information collected in the last 12 months, how it is used, the sources of the information, with whom it is shared, how long it must be retained (for erasure requests), to whom it is sold and the specific personal information about a requesting individual. Unless the business knows where its information is located it will not be able to fulfill these requirements of the CCPA.

Building a Data Inventory

Building a data inventory that includes the types of information that will be required for your disclosures under the CCPA is a rational first step towards compliance. To create a data inventory you will need to survey all aspects of your business, from Marketing to IT to HR to Vendor Management and all points where you receive information from any source and in any format. You may be surprised to learn all the places where personal information is hiding. The inventory should include:

1. A review of all areas of your business where personal information is received. This includes any type of personal information that you receive in any format, for example, through your website, forms at retail locations, mail and email, employment applications and related documents, call center recordings, vendor or service providers, landlords, tenants, marketing, closed-circuit TV, etc.
2. Identification of all categories of personal information you receive. The CCPA defines personal information broadly to mean information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer *or household*." It provides a non-exclusive list of examples of personal information including the usual contact information, IP, protected classification information (sex, ethnicity, race, etc.), biometrics, internet browsing information, products purchased or considered for purchase, geolocation data, academic and employment information and inferences drawn to create a profile about the individual to reflect preferences, attitudes, etc.
3. For each category of personal information identified, identification of the sources of the information. These could be directly from the individual, indirectly through a third party or from your own observations.
4. For each category of personal information identified, identification of all of the purposes for collecting the data and your uses of the data.
5. Identification of the length of time each category of information is legally required to be retained so that deletion requests can be honored properly.
6. Identification of all entities that are given access to the information, including whether a contract is in place with that entity, the purpose for such access and whether the entity may use the information for its own commercial purposes.
7. Identification of the location where the information identified is stored, in what format it is stored, and the person(s) responsible for maintaining the information.

Once you know what data you have and where it is, you will be able to use the data inventory to build out the disclosures required by the CCPA both in your public-facing privacy policy and in templates for your on-demand disclosure responses.

(For more information about CCPA and its ramifications, or for information about properly creating and orchestrating a crisis prevention plan around CCPA requests for information, please contact the authors.)

1 CCPA's requirements do not apply to "medical information" subject to the California Confidentiality of Medical Information Act (CMIA) or to "protected health information" collected by covered entities and business associates under the HIPAA Privacy, Security and Breach Notification Rules. Moreover, providers of health care subject to CMIA and covered entities subject to HIPAA are not covered businesses under CCPA if they maintain all patient information in the same manner they maintain "medical information" or "protected health information" subject to CMIA and HIPAA, respectively. CCPA also exempts information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act or the California Financial Information Privacy Act as well as other exemptions.

pillsbury