LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, MAY 23, 2022

MCLE

CPRA Series: Part IV

Data Processing Obligation

The California Privacy Rights Act ("CPRA") will significantly impact how entities process personal information requiring covered businesses to review and update their existing vendor agreements. The CPRA also includes additional requirements for specific data processing activities that may present heightened risks regarding consumers' data security and privacy. Part 4 provides an overview of these new requirements and includes practical advice for businesses to consider as they roll out their CPRA compliance programs.

Understanding the Relevant Terminology

As discussed in previous articles in this series, the term "business" refers to an entity "that collects consumers' personal information" and "determines the purposes and means of the processing of consumers' personal information." The CPRA uses this terminology to refer to what many other privacy regimes call the controller.

With the CPRA, external entities that process a business's personal information will fall into one of three categories: (i) service providers, (ii) contractors, (iii) third parties. The term "service provider" refers to persons that receive consumer personal information from/on behalf of a business, which carry out processing activities on behalf of a business for a business purpose under a written contract. One of the significant differences between the California Consumer Privacy Act ("CCPA") and CPRA is the CPRA's introduction of the term "contractor." This term refers to persons "to whom the business makes available a consumer's personal information for a business purpose" under a written contract. Unlike service providers, contractors do not carry out processing activities on behalf of the business. Thus, the distinction between the two appears to be the purpose for which personal information is disclosed, i.e., is the entity "processing" the information on behalf of the business or has the information been merely disclosed to the entity for an alternative purpose (e.g., a business disclosing records to an auditor that may include certain personal information). Persons that do not qualify as a covered "business," "service provider," or "contractor" are referred to as "third parties." Notably, selling or sharing (for purposes of cross context behavioral advertising) personal information with third-parties triggers disclosure requirements for covered businesses as well as consumer opt-out rights.

The term "contractor" is a welcomed change. Before the enactment of the CPRA, the CCPA forced many privacy practitioners to describe contractors as "restricted third parties" or "1798.140(w)(2) persons" —due to an unwritten and complicated exception. The CPRA eliminated that ambiguous language in the CCPA definition of third party and filled the logical gap by incorporating the "contractor" terminology and concept.

CPRA Contractual Requirements for Service Providers and Contractors

	Contractors	Service Providers
Selling & Sharing Restrictions	May not "sell" or "share" personal information.	
Processing PI	May not retain, use, or disclose personal information: (i) for any purposes other than those specified in the contract, or (ii) outside of the direct business relationship.	
Combining PI	May not combine personal information received from the business with other personal information received on behalf of another person or collected through its interactions with the consumer, except as otherwise permitted by statute or regulation.	
Sub-Processors	Must notify businesses when sub-processors are processing personal information and must bind these sub-processors to the same processing obligations.	
Complicance Certification	Must provide certification that the contractor understands the four restrictions listed above.	No certification requirement.
Compliance Monitoring	Must permit compliance monitoring by the covered person.	No compliance monitoring requirement.

Understanding these terms is essential for several reasons. The CPRA's opt-out rights apply to third parties but do not apply to contractors or service providers. Furthermore, subtle differences in the definitions and requirements for contractors and service providers (described below) may impact an entity's ability to process data.

Contract Requirements for Service Providers and Contractors

While the required contract provisions needed to establish service provider and contractor relationships are very similar, there are subtle differences that businesses must consider. As indicated in the chart below, the different contractual requirements revolve around compliance certification and monitoring. These differences seem to be driven by the CPRA drafters' desires to ensure checks are in place to govern the slightly broader range of processing activities in which contractors may engage. Businesses are not required to include these terms in their contracts with third parties.

New 1798.100(d) Requirements

In addition to the requirements discussed above, Section 1798.100(d) of the CPRA includes five items that must be included in the applicable business contracts. These requirements apply to third parties, service providers, and contractors (collectively, "Data Recipients"). Specifically, this new subsection requires agreements to:

(1) Specify personal information is sold or disclosed by the business only for limited and specified purposes;

(2) Obligate the Data Recipient to comply with applicable CPRA obligations, which includes providing the CPRA-level of privacy protection to covered information;

(3) Grant the business rights to take reasonable and appropriate steps to help to ensure that the Data Recipient uses the personal information transferred in a manner consistent with the business's CPRA obligations;

(4) Obligate the Data Recipient to notify the business if it determines that it can no longer meet its CPRA obligations; and

(5) Grant the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of personal information.

Other CPRA-Related Considerations for Data Processing

A. Audits and Risk Assessments

Section 1798.185(a)(15) of the CPRA requires the California Privacy Protection Agency (CPPA) to issue specific regulations for businesses "whose processing of consumer's personal information presents significant risk to consumers' privacy or security" under which such businesses must:

(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; and

(B) Submit to the CPPA on a regular basis a risk assessment with respect to their processing of personal information, including 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.

While specific examples of "significant risk" have yet to be provided, the CPRA states that the regulations should ensure both the "the size and complexity of the business" and "the nature and scope of processing activities" should be considered. Businesses in need of further instruction may also look to Europe's General Data Protection Regulation (GDPR) for guidance, which imposes a requirement on covered entities to conduct similar "data protection impact assessments" when data processing activities are likely to result in a "high risk to the rights and freedoms of natural persons."

B. Information Security

In addition to the aforementioned cybersecurity audit requirements, the CPRA requires that all covered businesses engaged in the collection of personal information "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."

Not surprisingly, the CPPA has not been tasked with further defining "reasonable security procedures" as what qualifies as reasonable will be unique to each organization, and will depend on factors such as the products and services offered (e.g., on-prem vs. SaaS solutions), nature of data collected, the size of the organization, available resources, and the like. As such, businesses should continue to rely on guidelines and frameworks when making decisions (e.g., NIST Cybersecurity Framework, Top 18 CIS Controls (previously the Top 20 CIS Controls), etc.). Notably, the California Attorney General has even provided its view that the Top 18 CIS Controls represent the "minimum level of information security that all organizations that collect or maintain personal information should meet," which suggests that such controls represent the baseline for "reasonable security procedures and practices," at least in California.

C. Disclosures Related to Automated Decision-Making

The CPRA requires the CPPA to issue regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology, including profiling and requiring businesses' response to access requests to include meaningful information about the logic involved in those decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."

While automated decision-making is not defined in the CPRA, the term profiling is defined to include "any form of automated processing of personal information […] 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."

In the absence of issued regulations, the CPRA does not directly obligate businesses to disclose their use of automated decision-making technology or provide any related opt-out rights. Regardless, given the direction in which privacy laws are headed (i.e., increased transparency and reducing the likelihood of discriminatory outcomes), businesses using automated decision-making technology should get ready. Steps businesses can take now include:

- Identifying the data used or created through automated decision-making technology;
- Creating summaries of the logic used for automated decision-making technology;
- Preparing policies and procedures explaining the likely outcome of these covered activities; and
- Creating procedures to allow for manual decision-making in instances where a consumer has exercised their opt-out rights.

Businesses that are heavily reliant on automated decision-making technologies may also want to consider adjusting their processes to include some level of human intervention. In Europe, under the GDPR, even a minimal amount of human intervention is sufficient to exempt a process that would otherwise be regulated as automated decision-making.

What's Next?

All covered businesses should begin reviewing their vendor contracts to determine whether amendments are needed to comply with the new contractual requirements discussed above. Covered businesses should also consider whether they are acting as a service provider, contractor, or third party in some contexts. For instance, a software provider may, on one hand, be a covered business when processing its employees' personal information (see Part One of this Series for further information about the status of the employee data exemption under the CPRA) and, on the other hand, be a covered service provider regarding the personal information it processes on behalf of its customers. In these instances, businesses should prepare contractual language that covers both roles, and may also want to clarify in its privacy policies its dual positions.

In some instances, contracts that arguably meet the CPRA's requirements should also be updated as a matter of best practice. For example, businesses with contracts containing broad obligations regarding the vendor's assistance with data privacy compliance matters should consider seeking more specific terms covering the Section 1798.100(d) obligations. Of course, contracts governing data-intensive processing activities should be the first priority. Businesses should also consider amending their standard template agreements or data protection addendums to address the CPRA's requirements.

Businesses should also begin evaluating the nature of their data processing activities to determine which new CPRA requirements may apply. In addition to updating contracts, initial efforts should focus on processing activities that may be considered high-risk, as well as processing that may constitute automated decision-making, bearing in mind the regulations are expected to address both of these issues so some flexibility in compliance procedures will be required.

Ron Raether, James Koenig *and* **Kamran Salour** *are partners;* **Sadia Mirza,** *and* **Graham Dean** *are associates and* **Edgar Vargas** *is an attorney at Troutman Pepper Hamilton Sanders LLP.*

Reprinted with permission from the *Daily Journal.* ©2022 Daily Journal Corporation. All rights reserved. Reprinted by ReprintPros 949-702-5390.