BCLP. Client Intelligent

Insights

THE CPRA DIGEST: CONTRACTING WITH "CONTRACTORS"

Aug 17, 2021

SUMMARY

On November 3, 2020, Californians voted to pass Proposition 24, expanding and modifying the California Consumer Privacy Act ("CCPA"), which came into force on January 1, 2020. The new California Privacy Rights Act ("CPRA") supersedes the CCPA and will be operative on January 1, 2023 (with a look-back period starting January 1, 2022). Until that time, the CCPA as currently written remains in effect. As we learned during the lead up to the CCPA, the time period to prepare for this type of comprehensive and complex legislation passes quickly, and companies need to begin their CPRA preparations sooner rather than later. In this installment of the CPRA Digest, we examine "contractors," a newly-added category of vendor, and the contracting implications of this classification.

As a general rule, entities that disclose personal information to other organizations trigger the Do-Not-Sell and sharing notice and opt-out rules under the CPRA, unless an exception applies. To this end, the CPRA adds "contractor" as a category of entities that a business may share personal information with without triggering the notice and opt-out requirements for sales and sharing. While the term "contractor" is new, it appears to be a refinement of the concept of an undefined type of vendor articulated in the CCPA and commonly referred to as a "non-third party."

A "contractor" is a person to whom the business "makes available" a consumer's personal information for a business purpose.[1] "Contractors" are distinguishable from "service providers" that "process personal information on behalf of a business."[2] In other words, "contractor" may be a more appropriate designation for an organization that receives personal information as part of providing a service to the disclosing organization (rather than receiving the information for its own commercial purposes) but is still not processing personal information solely on behalf of the business and/or that exercises autonomy over its use of personal information (e.g., a vendor engaged to provide an installment payment option on a retailer's e-commerce platform).

To fall within the scope of this definition, the CPRA establishes minimum contracting requirements. Specifically, a business must enter into a written contract which prohibits the contractor from:

- Selling or sharing the personal information.
- Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract, or as otherwise permitted by the CPRA.
- Retaining, using, or disclosing the personal information outside of the direct business relationship between the parties.
- Combining the personal information received from or on behalf of the business with personal information received or collected in other contexts.

These prohibitions apply to "service providers" as well, but a "contractor" must additionally (1) certify that it understands the forgoing prohibitions, and (2) permit the business to monitor its compliance with the contract through measures including: ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve months. By contrast, the certification obligation and compliance monitoring rights are not mandatory for contracts with "service providers."

These new unique contracting obligations put a greater burden on businesses to carefully consider their data flows with their vendors to ensure that the necessary terms are included in their written agreements to avoid triggering the notice and opt-out requirements for sales and sharing but do also provide clearer guidance for organizations engaging a vendor that does not fall neatly within the service provider definition.

Be sure to follow our CPRA Digest as we continue to examine other key aspects of the CPRA and steps that companies can undertake to begin addressing them. Our prior alerts are available here.

[1] Cal. Civ. Code Section 1798.140(j)(1). Business purposes include activities such as auditing, maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, etc. Section 1798.140(e).

[2] Cal. Civ. Code Section 1798.140(ag)(1).

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM

Goli Mahdavi

Co-Author, San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Christian M. Auty

Co-Author, Chicago

christian.auty@bclplaw.com
+1 312 602 5144
