Articles + Publications | August 5, 2024

Data Minimization Under the CCPA

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos

RELATED OFFICES

Hartford

The California Consumer Privacy Act of 2018 as initially adopted (or subsequently amended until 2020) did not contain the principle of data minimization. A requirement to minimize data collection was, however, added by the amendments effected by the California Privacy Rights Act of 2020 (the "CPRA"). With the effectiveness of those amendments, the California Consumer Privacy Act of 2018 (as amended, including by the CPRA, the "CCPA") joined the European privacy and U.S. healthcare privacy regimes in requiring data minimization. Although this article reviews the data minimization principle of the CCPA, it should be noted that other, subsequent state consumer privacy laws also include this principle; the California guidance is helpful for businesses subject to those laws as well.[1]

For context, Article 5, Section 1(c) of the General Data Protection Regulation of the European Union (the "GDPR") articulates the "data minimisation" principle that "Personal data shall be relevant and limited to what is necessary in relation to the purposes for which they are processed." Similarly, the Privacy Rule promulgated by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") includes a minimum necessary standard.[2] The HIPAA Privacy Rule generally requires covered entities to "make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

Consistent with the "data minimisation" principle of the GDPR and the "minimum necessary" standard of the HIPAA Privacy Rule, CCPA Section 1798.100(c) provides:

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.

Section 7002(a) of the Regulations promulgated by the California Privacy Protection Agency (the "CPPA") pursuant to CCPA Section 1798.100(c) expounds on the statutory requirement as follows:

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).

The data minimization principle of the CCPA applies to all processing of data by a business subject to the CCPA. On April 2, 2024, the CPPA issued Enforcement Advisory No. 2024-01 (the "Advisory") to provide guidance on the applicability of data minimization to CCPA consumer requests. The Advisory identifies data minimization as "a foundational principle in the CCPA," underscored by many aspects of the CCPA's implementing regulations. According to the Advisory, "Businesses should apply the principle of data minimization to every purpose for which they collect, use, retain, and share consumers' personal information." The Advisory names important functions served by data minimization, such as the reduction of risk of unauthorized access, and support for good data governance (including by expediting responses to consumer requests).

In one scenario offered in the Advisory, the CPPA considers a hypothetical consumer request to opt out of sales and sharing of personal information. According to the CCPA, if the business sells or shares information concerning the consumer's online activities, the business should not request more information (besides the consumer's name) from the consumer in connection with the request, and should honor it without verification. If, however, the business sells or shares other information, such as purchasing history, then the business may need to further identify the consumer, provided that the "minimum personal information" should be collected in connection with the identification. According to the CPPA, a driver's license might exceed this standard because, presumably, less sensitive information could be used.

The Advisory also considers a second hypothetical in which a consumer who does not have an account with the business requests deletion of personal information. Here, the business is advised to balance the sensitivity of the data to be deleted and the potential harm to the consumer caused by unauthorized deletion against the general principle of data minimization.

In the Advisory, the CPPA offers the following questions for consideration by a business in applying the data minimization principle to consumer requests:

- What is the minimum amount of personal information necessary for our business to honor a request to opt-out of sale/sharing?
- We already have certain personal information from this consumer. Do we need to ask for more personal information than we already have?
- What are the possible negative impacts if we collect additional personal information?
- Could we put in place additional safeguards to address the possible negative impacts?

These questions from the CPPA provide important guidance to businesses subject to the CCPA, as the CPPA can be expected to use the factors suggested by these questions outside the context of responding to a consumer request. Businesses subject to various other state consumer privacy laws and interested in good data governance would also benefit from considering these CCPA questions. These questions are instructive in considering any collection, use, sharing and retention of personal information. As noted in the Advisory, data minimization can help

mitigate data breach risks, and support data governance. Businesses applying the data minimization principle will collect, use, disclose and retain lower volumes of personal information, thereby streamlining the timeline and effort for data mapping, risk assessments, responses to consumer requests, and the investigation of and response to cybersecurity incidents.

—

[1] *See* Section 6-1-1308(c) of the Colorado Privacy Act; Section 6(a) of the Connecticut Data Privacy Act; Section 12D-106(a)(1) of the Delaware Personal Data Privacy Act; Chapter 4, Section 1(1) of the Indiana Consumer Data Protection Act; Section 6 of the Iowa Consumer Data Protection Act; Section 4(1) of the Kentucky Consumer Data Protection Act; Section 14-4607(B)(1)(I) of the Maryland Online Data Privacy Act; Section 8.2(a) of the Minnesota Consumer Data Privacy Act; Section 7(a) of the Montana Consumer Data Privacy Act; Section 12(a) of the Nebraska Data Privacy Act; Section 507-H-6.I(a) of New Hampshire RSA; Section 9.a(1)of the New Jersey Data Protection Act; Section 5(1)(b) of the Oregon Consumer Privacy Act; Section 47-18-3204(a)(1) of the Tennessee Information Protection Act; Section 541.101(1) of the Texas Data Privacy and Security Act; and Section 59.1-578.A of the Virginia Consumer Data Protection Act.

[2] 45 CFR 164.502(b), 164.514(d).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber