CLIENT ALERTS & INSIGHTS

California Privacy Protection Agency Issues First Enforcement Advisory; Addresses Data Minimization Concerns

APRIL 8, 2024

In its first ever enforcement advisory, the CPPA highlighted the key concept of data minimization-specifically focusing on excessive data collected when consumers make requests pursuant to their data privacy rights under the California data protection laws.

The days of minimal enforcement action under U.S. state data protection laws may soon be over. And the California Privacy Protection Agency's (the "CPPA") first enforcement advisory-Applying Data Minimization to Consumer Requests-may be a harbinger for things to come.

To date, California has been the only U.S. state to take significant enforcement action pursuant to the California Consumer Privacy Act (the "CCPA"), and even then, there has only been one substantive enforcement action under the CCPA from the California Attorney General (prior to the CPPA taking on the lead enforcement role).

The CPPA's first enforcement advisory may represent a turning of the page in U.S. data protection law from an era of new, unknown legislation to a period of enforcement.

Businesses should-if they have not already-ensure their privacy and security compliance programs are up-to-date and built out in accordance with the various U.S. state data protection laws.

The potential advent of increased advisories, guidance, and even enforcement action may turn out to be welcome news for businesses that have started to grapple with the nuanced-and at times ambiguous and overlapping-requirements set forth in the numerous U.S. state data protection laws. There are now well over a dozen states with omnibus data protection laws in place, from California to Texas, to Virginia to Colorado, and many more.

See Benesch's "U.S. State Privacy Laws" webpage for a full accounting of such laws and a high level overview of their overlapping requirements.

California Data Minimization Requirements

Data minimization is a common phrase thrown around when discussing data protection principles and has become commonplace in data protections both in the U.S. and around the globe.

Under the CCPA, businesses are required to configure their data collection and use such that the personal data collected is "*reasonably necessary and proportionate*" to achieve the purposes or which the personal data was collected or processed. The CCPA also permits use of personal data for purposes that are compatible such that a reasonable consumer would expect such ancillary processing.

The regulations set forth under the CCPA also shed light on what "*reasonably necessary and proportionate*" means. In deciding what is necessary and proportionate, a business shall weigh the following questions:

- What is the minimum personal data necessary to achieve the stated purposes?
- What are the possible negative impacts on the consumers in question posed by the data collection and use?
- Are there additional security safeguards that could be leveraged to address the possible negative impacts?

Based on the advisory and the regulations, if a specific data collection use case is risky from the perspective of the consumer, the amount of data collected and amount of time it is stored, should be smaller. Additionally, in such a case, the data should be protected via additional security measures.

In laymen's terms, data minimization means a business is only permitted to:

1. collect and use the minimum amount of data necessary for specific purposes (e.g., those purposes that are stated in that business's privacy notice); and
2. only retain / store such limited data set for the minimum period of time necessary for that specific purpose.

And even then, a business is required to ensure-as with any data collection under the CCPA-that reasonable and appropriate security measures are in place to protect the data.

There are also several other provisions of the CCPA that drive home the importance of data minimization, such as allowing consumers the rights to opt-out of the sale of their personal data or opt-out of the sharing of their personal data for targeted advertising purposes.

Data Subject Request Verification

The enforcement advisory, while touching on data minimization at a higher level, focuses on data minimization as applied to a business verifying a consumer privacy rights request.

Under the CCPA, a business is permitted to take reasonable steps to verify the identity of a consumer prior to granting or acting on that consumer's privacy rights request (for example, a request to delete, correct, or access their personal data). The CCPA's regulations stipulate that:

1. a business should, where feasible, try to match identifying information about a requestor to consumer personal data the business already holds (e.g., avoid asking for redundant personal data);
2. avoid collecting any sensitive categories of personal data (e.g., social security numbers) in its verification processes; and

3. only use such additionally requested information if necessary for the purpose of verifying a request, and not use the additional information for any purpose other than to verify the request.

In the enforcement advisory, the CPPA stated that it is "observing, however, that certain businesses are asking consumers to provide excessive and unnecessary personal information in response to requests that consumers make under the CCPA."

Practically, businesses need to ensure that such verification data is not commingled with other personal data a business generally collects and uses-the latter of which is likely subject to longer retention periods and other use cases. The verification data should only be kept for the period necessary to verify and act on the request-which is likely a shorter period of time.

In building out a consumer privacy rights request and verification process, the enforcement advisory implores businesses to consider the following:

1. What is the minimum amount of personal data necessary for the business to honor a request?
2. If the business already has certain personal data from the consumer, does the business need to ask for more personal data?
3. What are the possible negative impacts if the business collects additional personal data?
4. Could the business put in place additional safeguards to address the possible negative impacts?

Violations and Enforcement

As a reminder, violations of the CCPA can lead to $2,500 fines per violation or up to $7,500 fines per intentional violations involving the personal data of those under the age of 16. With regard to agency enforcement actions, there is no cure period provided. Meaning, as soon as the CPPA determines a violation has occurred, they can impose fines.

Importantly, the CCPA is unique in that it provides consumers with a limited private right of action allowing consumers to sue businesses for certain violations of the CCPA. The CCPA is still the only U.S. state omnibus data protection that allows any kind of private right of action. Under the CCPA, a consumer is permitted to initiate a civil action against a business that suffers a data breach (meeting the definition of California's data breach notification law) due to the business failing to implement and maintain reasonable and appropriate security procedures and practices.

Conclusion

The period of implementing and building out data protection compliance programs based on the new slate of U.S. state data protection laws is likely coming to an end. Now, businesses need to prepare for enforcement and regulatory action. Businesses will need to be nimble to adjust their existing data protection compliance programs to account for new guidance that comes out of enforcement advisories and inevitable enforcement actions.

As US states begin advising on and enforcing the slate of overlapping data protection laws that have come into force over the past few years, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.