THOMPSON HINE

Privacy & Cybersecurity Update

April 2024

CPPA Releases First Enforcement Advisory

On April 2, the California Privacy Protection Agency (CPPA) Enforcement Division issued Enforcement Advisory No. 2024-01, the first among several the agency expects to release this year. Enforcement Advisories seek to promote voluntary compliance with the California Consumer Privacy Act, as amended, and its implementing regulations (collectively, CCPA). This first Enforcement Advisory focuses on the CCPA's data minimization requirements in the context of consumer data privacy requests.

CPPA Enforcement Advisories

According to the CPPA, Enforcement Advisories are intended to "educate the public and encourage businesses to comply with the law to the benefit of all Californians, and address select provisions of the CCPA." The CPPA cautions that its Enforcement Advisories do not implement, interpret, or make specific the law it enforces or administers, nor do they establish substantive policy or rights, constitute legal advice, or reflect the views of its board. It further emphasizes that Enforcement Advisories do not provide options for alternative relief or safe harbor from potential violations. Instead, they call attention to selected areas of the law and provide examples of how businesses may review their practices to ensure compliance.

Scope of Enforcement Advisory No. 2024-01

Enforcement Advisory No. 2024-01 is titled "Applying Data Minimization To Consumer Requests." Data minimization is the principle that businesses should not collect, use, retain, or share more personal information than they need when processing consumers' personal data to reduce the risk that unintended persons or entities will access personal information (e.g., through data breaches) and to support good data governance.

The Enforcement Advisory states that "certain businesses are **asking consumers to provide excessive and unnecessary personal information**" in response to CCPA consumer privacy requests. It highlights areas where data minimization applies in the CCPA regulations and signals these four instances:

- Responding to opt-out preference signals
- Requests to opt out of sale/sharing
- Requests to limit the use and disclosure of sensitive personal information
- Identity verification in relation to consumer requests

The CPPA limits a business' collection, use, retention, and sharing of a consumer's personal information to that which **is reasonably necessary and proportionate** to achieve the purposes for which the personal information was collected or processed or for another disclosed purpose. The CCPA regulations clarify that this determination is based on the minimum personal information that is necessary to achieve the purpose identified, the possible negative impacts on consumers, and the existence of additional safeguards (e.g., encryption, automatic deletion of the personal information) to specifically address the possible negative impacts on consumers.

In discussing the concept of data minimization, the Enforcement Advisory underscores the term "**beyond what is necessary**" as it relates to the four instances noted above and outlines general rules to apply data minimization to identity verification that include:

- **Avoid collecting certain types of personal information** (e.g., Social Security number, driver's license number, financial account numbers, or unique biometric data) **unless necessary**
- **Avoid requesting additional information** from the consumer for purposes of verification
- If additional information is required, **use any new information solely for the purposes of verifying the identity** of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention and **delete new** personal information as practical **after processing the consumer's request**, except as required for record-keeping under the CCPA

Data Minimization Compliance Assessment

The Enforcement Advisory provides two examples to illustrate data minimization in the context of consumer requests. The first focuses on responding to requests to opt out of selling/sharing personal information. Notably, the Enforcement Advisory reminds businesses that the CCPA prohibits them from requiring consumers to verify their identity to opt out of sale/sharing or to make a request to limit. The second example applies data minimization to procedures for verifying a consumer's identity (to exercise deletion rights).

The examples present a series of self-assessment questions that businesses should consider when responding to consumer data privacy requests, summarized as follows:

- What is the minimum personal information that is necessary to achieve this purpose (i.e., identity verification) or to honor a request to limit/opt-out request?
- 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 posed if we collect or use the personal information in this manner?
- Are there additional safeguards we could put in place to address the possible negative impacts?

The Enforcement Advisory also provides questions businesses should consider when conducting identity verification in relation to consumer requests:

- To what degree of certainty (reasonable or reasonably high) do we need to verify the identity of the consumer? How sensitive is the information to be deleted and what is the risk of harm to the consumer posed by unauthorized deletion?
- Can we rely on the personal information on file, or is it necessary to request additional (sensitive) personal information to comply with the request? Is asking for this information to verify a request to delete an email address disproportionate and excessive?

Conclusion

Compliance with the data minimization principle is squarely within the CPPA's enforcement agenda and businesses should incorporate the recommendations presented in Enforcement Advisory No. 2024-01 to ensure that their business practices do not exceed collecting and processing consumers' personal data beyond what is necessary and proportionate under the CCPA.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com
Certified Information Privacy Professional/United States (CIPP/US)

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com