CPPA Enforcement Advisory No. 2024-01: Applying Data Minimization to Consumer Requests

APPLYING DATA MINIMIZATION TO CONSUMER REQUESTS

SUMMARY

- Data minimization is a foundational principle in the CCPA. Many aspects of the CCPA's implementing regulations underscore this principle.
- Businesses must apply 11 CCR § 7002(d)—in coordination with other applicable sections of the CCPA and its implementing regulations—for each purpose for which businesses collect, use, retain, and share personal information.
- Data minimization principles apply to the processing of consumers' CCPA requests.

ENFORCEMENT OBSERVATIONS

Data minimization is a foundational principle in the CCPA. Businesses should apply this principle to every purpose for which they collect, use, retain, and share consumers' personal information.

Data minimization serves important functions. For example, data minimization reduces the risk that unintended persons or entities will access personal information, such as through data breaches. Data minimization likewise supports good data governance, including through potentially faster responses to consumers' requests to exercise their CCPA rights. Businesses reduce their exposure to these risks and improve their data governance by periodically assessing their collection, use, retention, and sharing of personal information from the perspective of data minimization.

The Enforcement Division 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. The Enforcement Division reminds businesses to apply the data minimization principle to each purpose for which they collect, use, retain, and share consumers' personal information—including information that businesses collect when processing consumers' CCPA requests.

ENFORCEMENT ADVISORIES GENERALLY

Enforcement Advisories address select provisions of the California Consumer Privacy Act and its implementing regulations. Advisories do not cover all potentially applicable laws or enforcement circumstances; the Enforcement Division will make case-by-case enforcement determinations. Advisories do not implement, interpret, or make specific the law enforced or administered by the California Privacy Protection Agency, establish substantive policy or rights, constitute legal advice, or reflect the views of the Agency's Board.

Advisories do not provide any options for alternative relief or safe harbor from potential violations. The statutes and regulations control in the event of any conflicting interpretation. The Advisory provides the questions that follow as hypothetical examples of how a business might review its practices. Businesses should consult the statute, regulation, and/or an attorney before taking any action to ensure compliance with the law.

WHAT THE LAW AND REGULATIONS SAY ABOUT DATA MINIMIZATION

The CCPA's data minimization principle stems from the law's general purpose and intent that businesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared. *See* Prop 24, § 3(B)(3).

The CCPA states:

> "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."
>
> Civil Code § 1798.100(c) (emphasis added).

Underscoring this principle, the regulations explain:

> "[W]hether a business's collection, use, retention, and/or sharing of a consumer's personal information is **reasonably necessary and proportionate** to achieve the purpose identified … shall be based on the following:
>
> (1) **The minimum personal information that is necessary to achieve the purpose identified** …. For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.
>
> (2) **The possible negative impacts on consumers** posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.

> (3) **The existence of additional safeguards** for the personal information **to specifically address the possible negative impacts on consumers** …. For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards."

11 CCR § 7002(d) (emphasis added).

Additional CCPA regulations reflect the concept of data minimization, as shown in bold below:

- **Opt-out Preference Signals.** "The business shall not require a consumer to provide additional information **beyond what is necessary** to send the signal." 11 CCR § 7025(c)(2).
- **Requests to Opt-out of Sale/Sharing.** "A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information **beyond what is necessary** to direct the business not to sell or share the consumer's personal information." 11 CCR § 7026(c).
- **Requests to Limit Use and Disclosure of Sensitive Personal Information.** "A business shall not require a consumer submitting a request to limit to create an account or provide additional information **beyond what is necessary** to direct the business to limit the use or disclosure of the consumer's sensitive personal information." 11 CCR § 7027(d).
- **General Rules Regarding Verification.** In determining the method by which the business will verify the consumer's identity, the business shall:

> (1) "Whenever feasible, **match the identifying information provided by the consumer to the personal information of the consumer already maintained** by the business, or use a third-party identity verification service that complies with this section.
>
> (2) **Avoid collecting** the types of personal information identified in Civil Code section 1798.81.5, subdivision (d) [such as Social Security number, driver's license number, financial account numbers, or unique biometric data], **unless necessary** for the purpose of verifying the consumer…."
>
> 11 CCR § 7060(c) (examples added); and:

> "A business shall generally **avoid requesting additional information** from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall **only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention.** The business **shall delete any new personal information** collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101."
>
> 11 CCR § 7060(d).

FACTUAL SCENARIOS

Businesses should carefully review whether they are applying the data minimization principle in their collection, use, retention, and sharing of consumers' personal information. Below are two illustrative scenarios in which a business might encounter the data minimization principle: (1) responding to a consumer's CCPA request to opt-out of the sale/sharing of personal information; and (2) verifying a consumer's identity in connection with a CCPA request to delete personal information.

SCENARIO ONE: RESPONDING TO A REQUEST TO OPT-OUT OF SALE/SHARING

As a hypothetical example, Business A—which is covered by the CCPA—receives requests from consumers seeking to opt-out of the sale/sharing of their personal information. Business A is determining how to comply with those requests, including how much personal information to collect from consumers to process their requests.

The CCPA and its regulations speak directly to the right to opt-out of sale/sharing (Civil Code §§ 1798.120, 1798.135; 11 CCR §§ 7025, 7026, 7060(b)). Business A applies the data minimization principle as explained in Civil Code § 1798.100(c) and 11 CCR § 7002(d). Importantly, Business A does not require consumers to verify their identity to make a request to opt-out of sale/sharing:

> "A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license."
>
> 11 CCR § 7060(b).

To apply data minimization principles to these requests, Business A could start by asking itself the following questions consistent with 11 CCR § 7002(c)-(d):

- 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?

The information necessary to achieve the purpose of completing the consumer's request will depend on **how** Business A sells or shares personal information, as well as **what** information it sells or shares. For example, if Business A sells or shares a consumer's online activities only in the context of cross-context behavioral advertising, then Business A would not need additional information, such as name or email address, to comply with a consumer request to opt-out of sale or sharing made by way of an opt-out preference signal.

By contrast, if Business A sells or shares profiles of consumers that include both online activity and other information (e.g., purchasing history), then Business A might need the consumer to further identify themselves to apply the opt-out to more than just online activity. Relatedly, if Business A sells or shares purchase history, then asking for unrelated personal information, such as a driver's license, might exceed the "minimum personal information" necessary to comply with the request.

SCENARIO TWO: VERIFICATION OF A CONSUMER'S IDENTITY

As a second hypothetical example, Business B—which is covered by the CCPA—receives requests from consumers to delete their personal information. These consumers do not have accounts with Business B. Business B keeps consumers' names and email addresses on file and receives requests to delete personal information from consumers using their email address on file. Business B is determining how to comply with those requests, including how to verify consumers' identities.

Business B must establish, document, and comply with a reasonable method for verifying that the person making the request is the consumer about whom the business has collected information. (11 CCR § 7060(a).) Business B's purpose for processing the consumer's personal information is to verify that the consumer making the request is the same consumer about whom the business has collected personal information.

In reviewing its verification method, Business B evaluates whether it has complied with the data minimization principle, as well as whether the verification method complies with any regulations that speak specifically to verification (e.g., 11 CCR § 7060 (General Rules Regarding Verification) and in this case, 11 CCR § 7062 (Verification for Non-Accountholders)).

To apply data minimization principles to these requests, the business could start by asking itself the following questions, as set forth in 11 CCR § 7002(c)-(d):

- What is the minimum personal information that is necessary to achieve this purpose (*i.e.,* identity verification)?
- 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?

To help answer these questions, the business will look to regulations that explain the general rules regarding verification (specifically 11 CCR § 7060(c)(1)-(3)), and the rules for verification for non-accountholders accountholders (in this case, 11 CCR § 7062(d), which addresses requests to delete). These regulations help inform the § 7002 data minimization analysis.

As noted above, Business B has consumer names and email addresses. Business B could ask itself:

- The information to be deleted is a name plus email. 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?
- We have the email on file. Can we rely on the email address, or is it necessary to request a driver's license number or social security number in order to comply with the request? Is asking for this information to verify a request to delete an email address disproportionate and excessive?

For another consumer, Business B has a name and email address on file, and also stores photographs and documents associated with the name and email address. Consumers access their photos and documents by logging in with their email and password, and a code is sent to their email, which they then input into Business B's systems. Business B receives a consumer request from the email address on file, asking to delete all personal information.

In reviewing its verification method, Business B will evaluate whether it has complied with the data minimization principle, as well as whether the verification method complies with any regulations that speak specifically to verification (e.g., 11 CCR § 7060 (General Rules Regarding Verification) and, in this case, 11 CCR § 7061 (Verification for Password-Protected Accounts)). These regulations help inform the § 7002 data minimization analysis.

In this scenario, Business B could ask itself:

- Are the documents and photos we have on file sensitive information that should warrant a more stringent verification process than just asking for an email address? What is the risk of harm to the consumer if we act on an unauthorized request to delete?
- We have the email on file. Can we rely on the email address, or can it be spoofed? Is it necessary to use a more stringent verification process, such as requesting the consumer's driver's license number or a copy of the license itself? Is asking for this type of information to verify a request to delete disproportionate and excessive?
- We don't typically have driver's license numbers in our systems. What are the possible negative impacts posed to the consumer if we do collect driver's license numbers? What harm might result if there's a breach and the driver's license numbers are accessed?
- Are there additional safeguards we could put in place to address these possible negative impacts? How does our business interact with consumers? Can we have the consumer request and confirm a code in order to verify their identity in connection with their request to delete? Should we have the consumer request and confirm the code as a means of reauthenticating their identity?

ISSUED BY

Enforcement Division
California Privacy Protection Agency
Michael S. Macko, Deputy Director of Enforcement
April 2, 2024