How Much Data is Too Much? 4 Steps Businesses Should Take as California Focuses On Data Minimization Requirements

Insights
4.12.24

Businesses take heed: California state officials just warned that the law prohibits you from collecting unnecessary data and retaining data for longer than necessary. The California Privacy Protection Agency published its first Enforcement Advisory on data minimization under the state's hallmark data privacy law on April 2, focusing on a very specific context: when businesses respond to consumer requests under the California Consumer Privacy Act (CCPA). Here is what you need to know and the four key steps you can take to avoid over-collecting data when you respond to CCPA consumer requests – including from employees and job applicants.

What is Data Minimization and Why Issue an Enforcement Advisory?

While an Enforcement Advisory is not meant to interpret the CCPA or make new law, it nevertheless provides insight into what a likely priority of the Agency will be going forward. And the April 2 Enforcement Advisory is very clear in providing a warning to businesses.

The Agency appears to have the impression that businesses are requesting too much information from consumers when they submit a CCPA consumer request. As it states: "Data minimization is a foundational principle of the CCPA." This principle is undermined when you make it too hard for consumers to exercise CCPA rights that effectuate data minimization, or you ask for too much information to verify a consumer's identity.

Data minimization is premised on the CCPA requirement that a business's collection, use, retention, and sharing of consumer personal information be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." Whether the collection, use, retention, and/or sharing of personal information is reasonably necessary and proportionate to achieve the purpose identified is based on the following:

- The minimum personal information necessary to achieve the purpose identified, or any purpose for which the business obtains the consumer's consent (meaning a use of the data that you've disclosed to the consumer at or before you collected the data from the consumer, or that you can prove was consented to by the consumer);
- The possible negative impacts on consumers; and

- The existence of additional safeguards for the personal information to specifically address the possible negative impacts on consumers.

To illustrate the concept, the Enforcement Advisory highlights this principle as seen in the CCPA rules regarding opt-out preference signals (aka global privacy controls), requests to opt-out of the sale/sharing of personal information, requests to limit the use and disclosure of sensitive personal information, and the general rules regarding verification of a consumer's identity.

The Enforcement Advisory further provides two factual scenarios where a business should consider and implement data minimization: in a response to a consumer request to opt-out of the sale/sharing of personal information; and when verifying a consumer's identify in response to a CCPA request to delete personal information.

Data Minimization Through Opting Out of Sharing and Selling of Personal Information

In the first scenario, the Enforcement Advisory reminds businesses that you cannot require a consumer to verify their identity in connection with a request to opt out of the sale or sharing of consumer personal information or a request to limit the use and disclosure of their sensitive personal information. That means your process for receiving, processing, and responding to these two types of requests cannot include an identity verification step. While you may need additional information to effectuate the opt-out, this is *not* the same as verifying a consumer's identity. And, when you need additional information, you should ask for the minimum amount necessary to effectuate the request.

The Enforcement Advisory first posits the scenario of a consumer opting out of cross-context behavioral advertising through an opt-out preference signal. Certain web browsers enable users to set up such signals so that the browser sends an automatic signal to the website that the user has opted out of the sharing of data through cookies for targeted ad purposes. In such case, you would not need additional information to read, process, and comply with the out-out signal.

However, if you sold or shared personal information offline and were unable to connect the online user with their offline activities, you would need additional information to effectuate the offline opt-out. That being said, the information requested should only be sufficient to effectuate that offline request. Asking for unrelated personal information – for example, asking for a driver's license to opt-out of having a business sell a consumer's purchasing history – would likely be in excess of what you need (according to this Enforcement Advisory).

Data Minimization When Verifying a Consumer's Identity

In the second scenario, the Enforcement Advisory walks through an example of how you may apply the principle when receiving consumer requests to delete personal information. Here, the Agency did not provide any easy or suggested answers – instead, it put forward a series of questions

(without any suggested answers) that you can ask in evaluating what information to request when evaluating whether to delete consumer data.

Despite avoiding answers to its own questions, the questions themselves provide some insight into what you should consider when determining how to verify an identity:

- **Evaluate the harm of an unauthorized deletion to the consumer.** While the example focuses on destruction of information of sentimental value, you should also consider whether the destruction of information could have economic or other significant negative impacts. Where the potential harm to a consumer is on the higher end of the spectrum, more stringent verification will be required. Where the information to be deleted is not significant, you need not overcomplicate the verification process. The key takeaway here is that the verification process cannot be a one-size fits all approach.
- **Evaluate the harm of asking for additional, new information from the consumer.** If you ask for highly sensitive information such as a driver's license or social security number, the consumer is at risk of identity theft if a data breach occurs. While not addressed in the Enforcement Advisory, you should also ask yourselves how requesting information from consumers that you do not already have (and thus cannot verify) helps you confirm the identity of the consumer.

It is important to emphasize that what is not at issue is any harm to your business. The Agency's questions are consumer-centered, considering only the benefits and harms they face. When determining the appropriate verification process, you should view your processes through that lens.

Your 4 Next Steps: A Compliance Guide

In order to best position your organization for compliance, we recommend you consider the following four steps:

1. Review Your Practices

Review your mechanism for processing requests to opt out of selling/sharing of personal information and to limit the use or disclosure of personal information. If you are verifying identities to process these requests, you need to stop immediately. If you need additional information to figure out who a person is so that you can process the request (perhaps they have a common name!), you should only ask for the minimum amount of information needed to process or effectuate the request.

2. Determine if it's Time for Global Privacy Controls

If your website utilizes third-party cookies, pixels, beacons, tags, or other tracking technology or discloses data to third parties that is then used for targeted advertising, and does not currently process or accept Global Privacy Controls (GPCs) as an opt-out preference signal, you must get this set up now.

3. Ensure Your Verification Processes are on Point

Review how you are verifying consumer identities for Requests to Know/Access, Delete, and Correct. You ideally should be verifying identities based on information already in your possession. That requires you to look at what you have and tailor the verification questions you ask based on that data. While it may be easier to just ask for a copy of a driver's license or other government ID, you may end up collecting information which you do not already have (and information which is considered sensitive information under the CCPA to-boot), thus subverting the data minimization standards encompassed in the law.

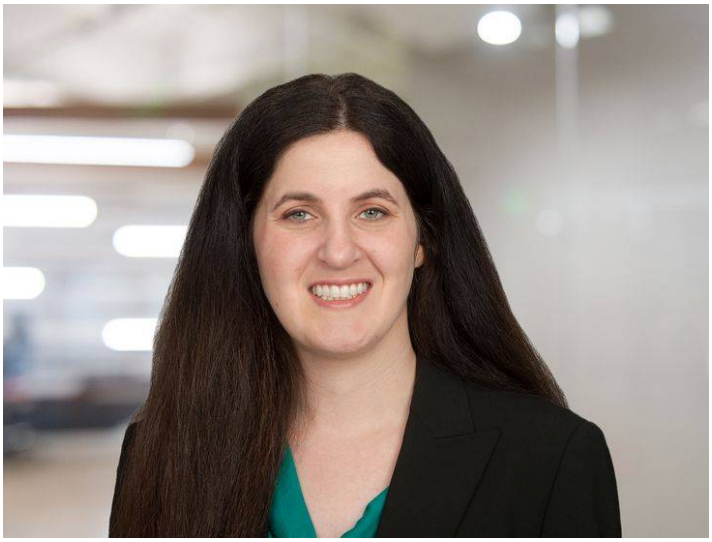
4. Purge Stale Data

While not addressed specifically in the Enforcement Advisory, the CCPA prohibits you from retaining personal information longer than you have a legitimate business purpose to do so. If your business does not have a data retention schedule or does not follow its data retention schedule, you should make it a priority. This includes ensuring that vendors that process and store data on your behalf also follow through with deletion of stale data. "Our vendor won't or can't delete the data" is likely not a good excuse anymore. The law requires stale data to be deleted, so there has to be a workable solution whereby data that you are legally responsible for can be deleted – wherever it resides.

Conclusion

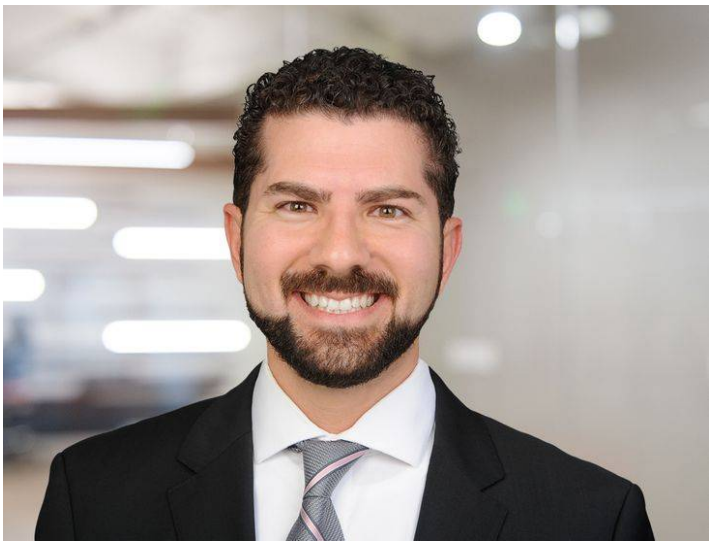
Fisher Phillips will continue to monitor CCPA obligations and enforcement efforts and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information directly to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or an attorney on the firm's Consumer Privacy Team. You can also visit our firm's CCPA Resource Center at any time.

Related People



Darcey M. Groden. CIPP/US

Associate
858.597.9627
Email



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Anne Yarovoy Khan
Of Counsel
949.798.2162
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills