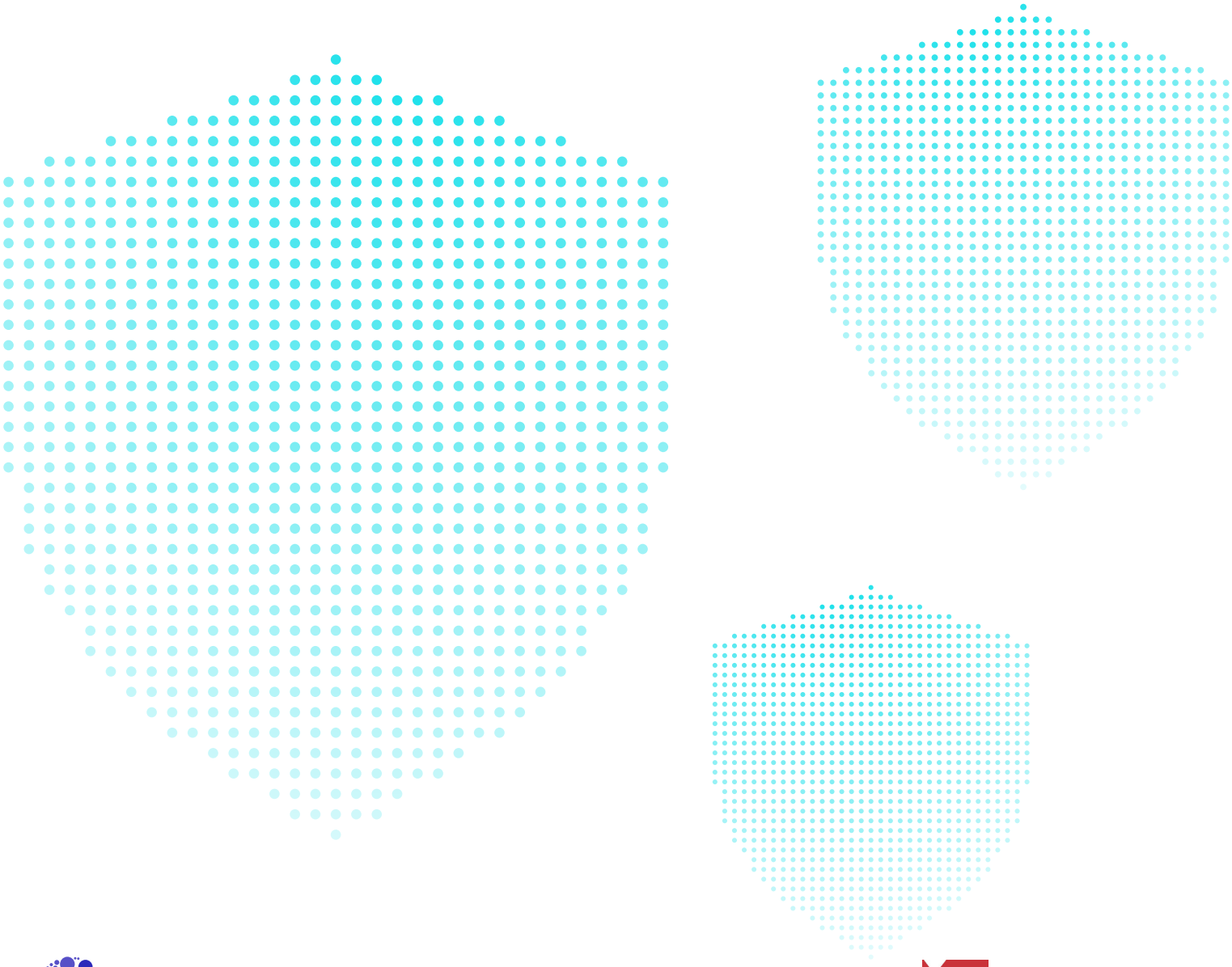
WHITE PAPER

Complying with the CCPA's Right to Deletion: A Strategic Approach



PRIVITAR

BakerHostetler

What's the challenge?

The California Consumer Privacy Act (CCPA) dramatically changed the regulatory landscape for privacy in the United States. Among the CCPA's many new requirements, one right is proving a particular challenge for many businesses: the right to delete.

The right to delete requires businesses that receive a verifiable consumer request to delete all the personal information they collected from that consumer, subject to certain exceptions. The business must also instruct its service providers to delete the consumer's personal information from the service providers' records. This can be difficult for large enterprises with complex data infrastructures and legacy systems. Many businesses are not aware of exactly what data they hold on an individual, where that data is stored, or how they have been shared throughout the business. This is compounded by the fact that some systems were not designed to delete data about just one individual, making the act of deletion itself a challenge. As a result, deletion requests can be extremely time consuming and expensive to comply with. In some situations, businesses may not be able to delete all relevant personal information or may not have the capability to confirm whether the information has been deleted.

Pseudonymization and de-identification may offer a path forward that facilitates compliance and moves businesses towards privacy by design.

What does the law require?

The CCPA regulations offer three ways a business may comply with a request for deletion:

"A business shall comply with a consumer's request to delete their personal information by:

- Permanently and completely erasing the personal information on its existing systems with the exception of archived or backup systems;
- Deidentifying the personal information; or
- Aggregating the consumer information."

Under the CCPA, de-identified means "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information:

1. Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2. Has implemented business processes that specifically prohibit reidentification of the information.
3. Has implemented business processes to prevent inadvertent release of deidentified information.
4. Makes no attempt to reidentify the information."

For many businesses, de-identifying data may be the most practical approach to deletion as it still allows the business to use data points on an individual basis.

What's the best way to deal with deletion requests?

Businesses developing their strategy for deletion requests should focus on three goals: effective compliance, cost minimization, and, where possible, residual data utility. For downstream systems, de-identification can offer better compliance, at a lower cost, while preserving some analytical utility in the data when compared to erasure.

Businesses often have core operational systems for which de-identification is not an option. If a marketing system is sending a customer an email, it needs to know the customer's name and email address. Typically, it's easier to find and delete data from these systems. Carrying out a consumer's right to delete often becomes complicated when data is transferred to downstream systems. Businesses may transfer copies of data from their core systems and repurpose them, perhaps placing the data into a data lake or development environment. Data may be copied into new tools, or even downloaded onto employees' local drives. However, this increases the difficulty in deleting data, as businesses may not be able

to track all the data about an individual and, even when they can, they may be unable to centrally control and delete the downstream data.

To counter these challenges, one option is pseudonymizing data whenever it leaves the business's core systems and before the business receives a request to delete. Generally, downstream systems are less likely to require identifiers like name and address so these values can be replaced with tokens. As long as tokenization is consistent and the format is preserved (for example, "Joe Blogs" is always replaced with "ghty lloiw"), data can still be linked and analyzed when needed. The business can store the mapping between the input value (Joe Blogs) and the token (ghty lloiw) in an encrypted token vault. This allows the business to re-identify "ghty lloiw" by looking up the input value in the token vault if necessary—for example, because of potential fraud or to use downstream analysis to provide the consumer with a new product or service. You can run all downstream applications using pseudonymous data, with re-identification actioned as applicable.

If the business subsequently receives a consumer's request to delete, a pseudonominization system allows the business to respond to the request by taking two simple actions: (1) erasing the identifying data from its core systems and (2) deleting the mapping for that individual in its token vault. This prevents the business from being able to re-identify the individual. That means that the data becomes fully de-identified, instead of only pseudonymized. This is better for compliance, as all data in downstream systems is affected immediately, rather than requiring the business to find and delete an individual's data throughout its systems. This solution is simpler and allows the business to use the de-identified data in the downstream systems for its analytical value, which would not be possible if the data had been fully erased.

Another approach some businesses have explored is using granular access controls that allow the business to remove employees' access to data upon receipt of a request to delete. This ensures the information can no longer be accessed but it does not actually remove the personal information from being stored in the system. This approach carries significant compliance risk because the business retains the ability to re-grant access, and it would therefore not constitute erasure, de-identification, or aggregation as required under the CCPA. Up-front pseudonymization helps to avoid these pitfalls.

Note that for pseudonymization to be effective, it must be carried out effectively. This means that all identifiers must be replaced with tokens as a matter of routine practice across all of the business's systems. If, for example, name, email, and phone number are all tokenized but an account number remains, then deleting the token vault mapping would not be sufficient because the data will still be considered personal information. It is, therefore, important to take care when choosing the pseudonymization method. Mature data mapping is important to ensure all relevant data elements have been identified and appropriately treated when leaving core systems.

Thinking about the future

In addition to supporting the right to delete, the approach outlined above has several other benefits.

First, it may mitigate risk to the business in the case of a data breach. Private rights of action under many state laws allow individuals to bring claims against businesses when their data has been breached. Often, however, state data breach laws exclude data that were properly encrypted or de-identified. Appropriately pseudonymized data with the token mapping held in an encrypted token vault can provide significant protection against such claims.

Second, routine pseudonymization supports businesses looking ahead to the new CPRA requirements that come into effect on January 1, 2023. Among other changes, the CPRA explicitly requires data minimization and storage limitation. Pseudonymizing data when it leaves core systems supports data minimization and allows businesses to more easily delete personal information

after an appropriate period of time to comply with the storage limitation principle. The same approach used for deletion requests can be applied to storage limitation requirements.

And finally, California is no longer the only U.S. state with a comprehensive privacy law. In 2021 Virginia and Colorado passed their own laws – the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA) – that will come into effect in 2023. Both the VCDPA and CPA encourage pseudonymization by exempting pseudonymized data from certain consumer rights, provided that the data is kept separately under appropriate technical and organizational controls. This means businesses have fewer obligations under the VCDPA and CPA for data they have pseudonymized.

This direction towards encouraging pseudonymization and then deleting token vault mapping where needed isn't just the path in the United States. It can also be seen in the EU under the GDPR. The approach was reviewed in a case by the Austrian Data Protection Authority, which concluded that fully anonymizing personal information can be considered erasure under the GDPR.

Overall, making the decision now to pseudonymize data when it leaves core systems reduces compliance risk and enables low-cost, high-efficacy approaches to the growing complexities involved when businesses must delete data. With data deletion requirements on the rise, acting now can help avoid future headaches.

Authors

Whitney Schneider-White, Associate, BakerHostetler
Whitney Schneider-White advises clients on domestic and global privacy, data protection and information governance issues. She provides practical, innovative solutions to her clients navigating the consistently evolving privacy and data protection landscape.

Justin Yedor, Associate, BakerHostetler
Justin Yedor specializes in partnering with clients to develop creative solutions to data privacy challenges. He is a thought leader on California privacy law, and a go-to advisor on the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

Guy Cohen, Privitar Policy Advisor
Guy joined Privitar in 2016, prior to which he worked in the UK Civil Service, in the Department of Health, the Cabinet Office and HMRC. Guy has been a fellow at Cambridge University's Centre of Science and Policy, a member of the Royal Society Privacy Enhancing Technologies Working Group, and the technical editor for the IEEE Data Privacy Process Standard.

About BakerHostetler

With scores of highly ranked attorneys across multiple practice areas, BakerHostetler helps clients around the world address their most complex and critical business and regulatory issues, delivering sophisticated counsel and outstanding client service. The firm has six core practice groups – Business, Digital Assets and Data Management, Intellectual Property, Labor and Employment, Litigation, and Tax – comprised of more than 1,000 lawyers located coast to coast. For more information, visit www.bakerlaw.com

BH BakerHostetler

About Privitar

Privitar empowers organizations to use their data safely and ethically. Our modern data provisioning solution builds collaborative workflows and policy-based data protection into data operations. Only Privitar has the right combination of technology, domain expertise, and best practices to support data-driven innovation while navigating regulations and protecting customer trust.

For more information, visit www.privitar.com

PRIVITAR

Published 7/22. Reference: P1007.2-WP-CCPA-Right-to-Delete-DP