ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

FEBRUARY 9, 2023

Secure Data Disposal and Data Minimization

by *Kim Peretti* and *Wevine Fidelis*

Data minimization, data retention, and secure data disposal have become priorities for 2023. Now more than ever, corporations are facing increased regulatory attention on data disposal practices from the Federal Trade Commission (FTC). Data disposal is also increasingly necessary to stay compliant with changing local and global data privacy regulations, including the California Privacy Rights Act (CPRA), which has adopted data minimization requirements and went into effect January 1, 2023. In addition, retaining unnecessary data can quickly become a heightened risk in today's cyber threat landscape, where ransomware actors target large data repositories for data encryption and exfiltration in cybersecurity incidents. With these various considerations at play, it is critical for organizations to review their secure data disposal strategies and enhance them where appropriate.

Federal Regulatory Frameworks

In the United States, the FTC has taken the lead through clear guidance and enforcement activity to establish the importance of secure data disposal strategies.

Federal Trade Commission guidance

On June 30, 2015, the FTC released *Start with Security: A Guide for Business*, which provided important guidance on data retention and secure data disposal practices, including: (1) "don't collect personal information you don't need"; (2) "hold on to information only as long as you have a legitimate business need"; and (3) "don't use personal information when it's not necessary." The FTC's *Start with Security* guidance draws from a 2005 enforcement action involving a company's 30-day retention period for certain payment information, which the FTC deemed longer than necessary because it violated payment card rules. The FTC found such storage of personal information was an unreasonable data security practice and that businesses should only hold on to consumer information if they have a "legitimate" business need.

On July 28, 2017, the FTC expanded on *Start with Security: A Guide for Business* with the "Start with Security – And Stick with It" blog post. The 2017 post expanded on the same principles as the *Start with Security* guidance and reiterated that a business should not collect sensitive information that it does not need. Finally, a business should continually review the data it maintains and adopt practices to determine whether such data is still needed or should be securely disposed.

Federal Trade Commission enforcement activity

In a 2019 enforcement action against InfoTrax Systems L.C., the FTC described the company's failure to implement "a systematic process for inventorying and deleting consumers' personal information … that is no longer necessary" as an unreasonable data security practice. In the consent order, the FTC required the company to implement specific policies and procedures to inventory the personal information collected on the company's network and create a system to delete personal information that is no longer necessary.

As recently as October 24, 2022, in a consent order against Drizly LLC and its CEO related to the company's alleged security failures in connection with a 2020 data breach, the FTC highlighted the importance of complying with data minimization principles to reduce the company's data footprint. Specifically, the FTC ordered Drizly to display on its website and applications its data retention schedule, explain why the company collected the consumer information and why the company needs the information, and provide a timeframe for deletion. This additional undertaking went above and beyond any prior understanding of transparency for data retention schedules.

Further, the order mandated data destruction within 60 days of the order. This required Drizly to delete or destroy all data that was not being used or retained in connection with providing products or services to customers and to provide a written statement to the FTC to confirm that all such data had been deleted or destroyed, including providing the specific categories of data removed. Considering the security incident led to exfiltration of more than 2.5 million consumers' personal information, this appears to be an onerous task to achieve within a brief, 60-day period. Drawing from its *Start with Security* guidance, the FTC reiterated the need for the company to refrain from collecting personal information that is no longer necessary for the purposes outlined in the data retention schedule.

International

The European Union (EU) General Data Protection Regulation (GDPR) has provided the leading international regulatory guidance on secure data disposal practices, which has already influenced the CPRA. Under the EU GDPR, Article 5 has codified six data principles related to processing of personal data, which provide the framework on how personal data must be processed. The first principle, under Article 5(1)(b), is purpose limitation, which provides that personal data may only be collected for specified and legitimate purposes and must not be processed in a manner that is incompatible with those purposes. The second principle, under Article 5(1)(c), is data minimization, which requires personal data to be relevant and limited to what is necessary for the purposes for which the data is processed. Under this requirement, companies are required to carefully consider whether collected data is necessary or just excessive. The final requirement, under Article 5(1)(e), is data retention, which requires companies to keep personal information for no longer than necessary for the purposes for which the personal information was initially processed.

State Regulatory Efforts

State efforts in regulating data disposal and minimization currently take two approaches. First, while state privacy laws generally do not set specific data disposal requirements, the CPRA has introduced new legal requirements for secure data disposal practices as of January 1, 2023. The second approach includes state data security laws focused on the secure disposal of records containing personal information.

California Privacy Rights Act

While the need to implement secure data disposal practices has grown increasingly prevalent across industries, state privacy laws generally do not set specific data disposal requirements. However, with the CPRA, which amends and expands the CCPA, California introduced three core GDPR principles into U.S. state law for the first time. The CPRA sets new standards for secure data disposal practices with the following requirements: data minimization, purpose limitation, and limited retention.

Data Minimization

First, the CPRA mandates data minimization, which requires companies to minimize data collected at the outset. Specifically, the CPRA prohibits the retention of a California resident's personal information for longer than is "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." This new requirement prompts businesses to continually evaluate their data collection practices and determine the purposes for which data is collected and processed. Businesses must identify and eliminate any unnecessary data collection and confirm that data collection remains compatible with the disclosed purposes.

Purpose Limitation

Second, the CPRA adopts the purpose limitation principle, which builds on data minimization to encourage transparency to consumers when their data is no longer being used for the stated purpose. The CPRA requires a business to inform consumers of the purpose of data collection in its privacy statements or other notices. A business may not process personal information for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which such personal information is processed, unless with the consumer's consent or as permitted by law. Notably, if a new use is proposed that is not compatible with prior disclosures, a business must provide new notice to consumers at collection. Under this new requirement, a business must develop a process for maintaining visibility over internal data uses and obtain pre-approvals for new use cases.

Limited Retention

Third, the CPRA requires limited retention in order to prevent businesses from holding data indefinitely without providing any justification for doing so. Under this new requirement, businesses would be required to inform consumers, at or before the point of collection of personal information, of the "length of time the business intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period." Effectively, the CPRA now requires businesses to disclose retention periods for various categories of personal information and to properly dispose of personal information once it exceeds the specified retention period. Further, this requirement expands on data minimization and limited retention principles because it requires businesses to monitor their maintenance of data and to remove personal information from their systems when that information is no longer necessary for the disclosed purposes or exceeds the applicable retention period.

Notably, now that the CPRA has taken effect, the CCPA's exemption for employee-employer data and business-to-business (B2B) data no longer applies. Accordingly, employers and B2B companies must bear in mind that the foregoing requirements under the CPRA will apply and expand the amount of data in scope.

State data security laws

While secure data disposal strategies through general state privacy laws are still in their infancy, several states have already enacted or proposed targeted legislation that governs data disposal. At least 35 states, including D.C. and Puerto Rico, have enacted laws that require private entities to securely destroy or dispose of personal information, or otherwise make it unreadable or indecipherable. These laws generally require businesses to refrain from storing data that is no longer needed for legitimate business purposes and to securely destroy or dispose of records containing personal information by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable by any means.

There is some slight variation among the states on which specific categories of personal information may be covered by these laws (for example, some states are limited to social security numbers while others cover additional categories of personal information). Though no state has implemented specific retention periods for any category of personal information, all are consistent with the notion that businesses must securely dispose of personal information once the information is no longer needed for a legitimate business purpose.

For example, New York's SHIELD Act requires that businesses "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data." It further requires companies to "dispose[] of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed." The data security program should include specified administrative, technical, and physical safeguards.

There have already been enforcement actions for these provisions. In 2020, a vision care company settled with the New York attorney general for $600,000 after failing to implement appropriate security measures that led to a breach impacting 2.1 million individuals. Specifically, according to the settlement order, the company (1) failed to implement multifactor authentication for the affected user account; (2) failed to implement reasonable safeguards for password management; and (3) had unreasonable data retention safeguards. Further, the attacker gained access to an employee email account containing emails and attachments dating back six years. The New York attorney general found "it was unreasonable to leave personal information in the affected email account for up to six years rather than to copy and store such information in more secure systems and delete the older messages from the affected email account," given the foregoing unreasonable protections.

The New York State Department of Financial Services also found that the company failed to implement a sufficient data minimization strategy and proper periodic disposal process for nonpublic personal information (NPI) to minimize the amount of NPI accessible to the threat actor in the shared mailbox, which contained old data that was accessible to the threat actor.

Key Takeaways

While the regulatory approaches vary at the international, federal, and state levels, there are common themes found throughout all approaches that can guide compliance efforts. Companies may wish to implement the following practices to comply with data minimization and secure data disposal requirements.

- **Evaluate Data Collection Practices:** Companies should begin assessing their current data collection practices to identify opportunities to minimize the collection of data at the outset. A company may elect to create a comprehensive data inventory that details the categories of personal data collected, the business purposes for the collection, how and where such data is processed, the recipients or categories of third parties that have access to the data, and the applicable retention periods.

- **Analysis of the Necessity and Purpose of Data Elements:** Once a company understands the data elements it collects, companies should perform an analysis of the necessity and purpose of each data element. This analysis will help the company to confirm that each data element collected is being processed in a manner that is consistent with the purposes for which the personal information was initially collected.
- **Maintain Visibility over Internal Data Uses:** A company should maintain visibility over its internal data uses to confirm when a new proposed data use is incompatible with prior disclosures. A company has the obligation to provide new notice to allow consumers to affirmatively consent to the new use of their personal information. In order to properly monitor, a company may want to develop an internal process to maintain visibility over new products and proposed new data uses in order to ensure it obtains the required pre-approvals for new use cases.
- **Review Retention Schedules:** Once the categories of personal information collected are identified and the company understands the purpose for such collection and the applicable retention periods for the data, a company can update its data retention schedules and privacy policies. The retention schedule and privacy policy should adhere to the legal obligations surrounding the maintenance of data. The company can then appropriately monitor its data and ensure the necessary data is properly removed from its systems at the end of the stated retention period.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**:

Kimberly Kiefer Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Daniel J. Felz
+1 404 881 7694
daniel.felz@alston.com

Katherine Doty Hanniford
+1 202 239 3725
kate.hanniford@alston.com

Amy Mushahwar
+1 202 239 3791
amy.mushahwar@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333