BCLP. Client Intelligent

Insights

THE CPRA DIGEST: DATA MINIMIZATION

Jan 06, 2021

On November 3, 2020, Californians voted to pass Proposition 24, expanding and modifying the California Consumer Privacy Act ("CCPA"), which came into force on January 1, 2020. The new California Privacy Rights Act ("CPRA"), supersedes the CCPA and will be fully operative on January 1, 2023 (with a look-back period starting January 1, 2022). Until that time, the CCPA as currently written generally remains in effect. As we learned during the lead up to the CCPA, the time period to prepare for this type of comprehensive and complex legislation passes quickly, and companies need to begin their CPRA preparations sooner rather than later. In this installment of the CPRA Digest, we discuss the addition of purpose limitation and data minimization requirements and the implications for organizations trying to anticipate the impact of the CPRA.

Data minimization – a core principle under GDPR[1] but not mandated under the CCPA – is now effectively required under the CPRA. Specifically, the CPRA bars businesses from collecting more personal information than "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed . . . ."[2] In addition and like the GDPR and other omnibus privacy laws, the CPRA also requires that a business "shall not retain a consumer's personal information or sensitive personal information . . . for longer than is reasonably necessary" for the purpose for which it was collected.[3] Taken together, these requirements mean that companies will need to carefully evaluate what data they collect and the purpose of the collection with an eye towards cutting out unnecessary data collection. Business must also implement measures to remove such information from their systems once it is no longer needed for such purposes.

This will be a familiar restriction for businesses that have worked to tackle these requirements as part of their GDPR or broader privacy compliance efforts. For those businesses, procedures implemented for GDPR can be extended to data collected about California consumers. For businesses that have not taken this compliance step and even for those that have, this may be a burdensome requirement.

In any event, there are pros and cons companies should be ready for as they decide how to approach the issue. As the commercial value of personal information grows and companies seek to maximize the value and volume of their data about consumers and other individuals, privacy

teams may face resistance in efforts to either minimize data collections at the outset and/or destroy or purge systems of personal information already collected. They should plan to work with these teams to help them understand these obligations and shape data collection efforts to achieve a balance between commercial and privacy considerations. Moreover, such efforts can help ease the burden of complying with other requirements under the CCPA and CPRA, such as complying with consumer rights requests, and reduce the risk and scope of issues such as data breaches. Helping internal stakeholders understand these benefits may also ease resistance to changes in data collection practices.

To actually operationalize the principle of data minimization, companies must understand what personal information they collect and maintain and the underlying purposes for such collection. While the CPRA does not require businesses to maintain written documentation of a data inventory, the development of a comprehensive data inventory (also sometimes referred to as a data map or data flow diagram) is a necessary step in understanding such data flows. Such records can be useful in achieving compliance with other aspects of the CPRA, such as facilitating consumer rights requests and serving as the baseline for accurate privacy notifications. But the net effect of the enactment of CPRA is that businesses will be required to have a functional data inventory.

A basic data inventory details the categories of personal data collected, the categories of data subjects from whom data is collected, the purposes for the collection, the categories of recipients of the data, and the applicable retention periods. It is also important to identify the systems or applications on which personal information collected and determine whether such systems or applications are maintained internally or externally. Finally, consider appointing an internal owner of the systems (for example, data storage/backup may be “owned” by IT) charged with periodically updating the inventory. Once there is organizational understanding regarding the data that is collected, the purpose for the collection, and how long various data elements are retained, businesses will be in a position to understand what personal information must be collected to achieve the relevant purposes and to examine the retention periods for various data elements and implement a data retention policy to meet the data minimization requirements of the CPRA.

Conducting a data inventory is a laborious endeavor, such that companies should not delay in kicking off these efforts. However, because data minimization is a requirement under the GDPR, significant progress has been made over the last few years in making the creation of data inventories more efficient. That practical experience should be leveraged for compliance with the CPRA. In addition, the upfront cost and allocation of resources to conduct a data inventory is easily offset by the potential penalties that businesses face if they operate in violation of the CPRA.

Be sure to follow this series as we continue to examine other key aspects of the CPRA and steps that companies can undertake to begin addressing them.

For other articles in this series, click below.

The Expanded Private Right of Action under the CPRA

California Passes New CPRA Privacy Regulation

1. Under GDPR, the data minimization principle requires entities to process only “adequate, relevant and limited” personal data that is “necessary.” GDPR Article 5(1)(c).

2. CPRA, Section 1798.100(c).

3. CPRA, Section 1798.100(a)(3).

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448
