Is your privacy policy a liability? California OAG releases CCPA enforcement guidance

Kate Campbell
414.287.9529
kcampbell@gklaw.com

Lillie L. Conrad
920.831.6356
lconrad@gklaw.com

Justin P. Webb
414.287.9527
jwebb@gklaw.com

As we move into the second year post-California Consumer Protection Act (CCPA), it is critical that your privacy policy is accurate, transparent and comprehensive. With new privacy laws taking effect in 2023, like the California Privacy Rights Act (CPRA), the Virginia Consumer Data Protection Act and the Colorado Privacy Act, privacy policy compliance will only become more challenging. Non-compliance with these laws and regulations may create a serious liability for your business.

With respect to CCPA, the California Office of the Attorney General (OAG) has been busy providing additional guidance on the law as well as CCPA regulations, including releasing a summary of recent enforcement actions. This summary gives companies insight into the regulatory data privacy risks they may be facing, as well as a roadmap to help correct minor issues that may give rise to regulator inquiry or enforcement action, or a consumer complaint. The OAG also updated its Frequently Asked Questions (FAQ) document, specifically noting that businesses must recognize technology known as the Global Privacy Control (GPC) to honor "Do Not Sell" requests and launched a new tool that allows consumers to report "Do Not Sell" violations.

CCPA enforcement summary

Upon receipt of a notice from the OAG of non-compliance with CCPA, a business or service provider has 30 days to cure any non-compliance before an enforcement action will be initiated. The summary of recent enforcement actions highlights common violations that appear across industries, including:

- Non-compliant privacy policies and the failure to inform consumers about their rights and how to exercise them
- The failure to provide adequate notice to consumers about how personal information is collected, used or sold
- The absence of a compliant "Do Not Sell My Personal Information" button or incorrect functionality of the button
- Insufficient, non-compliant or overly burdensome identity verification processes, including processes that are unclear or ask for too much documentation
- The failure to ensure contracts with service providers contain CCPA-required provisions
- The mis-categorization of entities as service providers under CCPA

Global Privacy Control requirements

The CCPA FAQ was recently updated with additional requirements for entities subject to CCPA with respect to the GPC. GPC a lesser known standard available on websites or as part of certain browsers used to communicate a

user's "Do Not Sell" request to the website operator. While the GPC is not referenced in the CCPA or accompanying regulations, the FAQ document now states that a request made by a consumer through the GPC "must be honored by covered businesses as a valid consumer request to stop the sale of personal information." Notably, the recently released enforcement examples build upon the inclusion of the GPC requirement in the FAQ document, with an example describing non-compliance with CCPA arising from the failure to properly process consumers' requests to opt out submitted via "a browser extension that signaled the GPC."

Given the recent updates to the FAQ and the inclusion of requirements related to GPC, it is important for entities subject to CCPA to ensure that they fully understand the GPC and are providing simple, legally compliant methodologies for consumers to exercise their "Do Not Sell" rights, including through the GPC.

OAG introduces new Consumer Privacy Interactive Tool

The California OAG also introduced a new Consumer Privacy Interactive Tool that consumers can use to submit a complaint to entities subject to CCPA if the entity does not have an easy-to-find "Do Not Sell Personal Information" process or link. The Consumer Privacy Interactive Tool walks a consumer through several questions and then creates an email notice that the consumer can send to the allegedly non-compliant entity. A copy of the consumer's submission to the Consumer Privacy Interactive Tool is also sent to the OAG. Keep in mind that receipt of a consumer's complaint may trigger the CCPA's 30-day period to cure any non-compliance.

It is also important to note that the Consumer Privacy Interactive Tool cannot confirm the veracity of the consumer's complaint, so it could be used for abuse or give rise to over-reporting of alleged non-compliance. Entities subject to CCPA would be wise to review their policies and procedures regarding data subject requests under CCPA and consider updating them to include a process for assessing a consumer complaint through the Consumer Privacy Interactive Tool. Where the entity receives a valid complaint of non-compliance, the updated policies and procedures should ensure that the entity has a process to rectify such non-compliance within 30 days.

Monitor CCPA, CPRA and other privacy law developments closely

As the interpretation and enforcement of CCPA evolves, entities subject to CCPA should monitor and, where necessary, evolve their privacy program in response to updates to the CCPA regulations and the CCPA FAQ document as well as enforcement actions and litigation driven by CCPA. The privacy landscape will only get more complicated in the next 16 months with the CPRA effective date fast approaching and new privacy laws in Colorado and Virginia on the horizon.

For more information on this topic, or to learn how Godfrey & Kahn can help, contact a member of our Data Privacy & Cybersecurity Practice Group.