CCPA 12-Month Compliance Series Part 5: Responding to Consumer Requests

At the core of complying with the CCPA is knowing how to deal with consumer's requests with respect to any of the eight rights regarding their personal information (PI), which are:

1. An abbreviated right to disclosure regarding PI collected (§1798.100)
2. An expanded right to disclosure regarding PI collected (§1798.110(a))
3. Right to disclosure regarding PI sold or disclosed for a business purpose (§1798.115)
4. Right to opt-out of sale of PI (§1798.120)
5. Right to opt-in for sale of minor's PI (§1798.120(c))
6. Right to deletion of PI collected (§1798.105)
7. Right to access PI (§1798.100(d))
8. Right to not be discriminated against (§1798.125)

A business must provide at least two designated methods, including a toll-free telephone number and a website address (if it has a website), for consumers to submit the requests. §1798.130(a)(2). Companies with websites should take care to ensure that requests made through the website are routed to a centralized location, and that the person responding to the requests is properly trained on how to do so. We have seen companies that failed to do this have problems complying with consumer requests made under the GDPR, by leaving some requests unaddressed or addressing them in inconsistent ways. At the outset, a business needs to ensure that the consumer request is "verifiable"; that is, the consumer, himself or herself, is making the request. The statute does not specify exactly *how* a business should verify a consumer request and indicates that the Attorney General's Office should adopt regulations specifying how to do so. Given that the regulations may not be adopted in sufficient time for businesses to be able to operationalize them prior to the effective date of January 1, 2020, businesses should consider implementing methods, such as two-factor authentication and blockchain technology now. This way, come January 1, 2020, they can be reasonably confident that they are not disclosing or delivering PI to someone other than the person to whom the PI belongs. If a request is not verifiable, then the business should not disclose the PI. There are other reasons why PI need not (or should not) be disclosed or delivered, as well. For example, a business need not disclose PI if the individual has submitted rights requests more than twice in the preceding 12-month period, if a request relates to PI collected more than 12 months prior, or fulfilling the request would infringe the rights and freedoms of other individuals, etc. Once a business verifies the request and determines that no defenses apply, it should know exactly what it is obligated to produce, and the response needs to satisfy the method and timing of delivery as specified in §1798.130(a)(2). Establishing procedures to implement obligations relating to consumer rights will allow your company to minimize both business disruption and risks in connection with CCPA enforcement when the Act becomes effective on January 1, 2020.

Authors

Gabriella Gallego

Associate
GGallego@perkinscoie.com 650.838.4815

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog