MINTZ

The Sun is About to Set on Temporary CCPA/CPRA Exemptions: Employers Get Ready

September 14, 2022 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

If you've relied on the temporary "exemption" for employee/applicant and business-to-business (B2B) personal information under the California Consumer Privacy Act (CCPA), those exemptions will expire on January 1, 2023. The California legislature adjourned on August 31 for the 2022 session without adopting legislation to extend those exemptions, and therefore, absent a special legislative session, they will sunset on December 31.

Also, the **California Privacy Rights Act (CPRA) amendments** will take effect on January 1, 2023 and that means that if your company is a "business" under CCPA/CPRA (see **here** for general information on CCPA), employers of California residents will need to include employment-related data in privacy compliance programs. For many businesses, that may mean a complete overhaul of privacy and compliance practices to accommodate workforce members.

Effect on Employers

Come January 1, 2023, your California workforce members will have privacy rights in CCPA/CPRA (subject to certain exceptions) and you will need to be prepared to respond:

- Right to Know: includes right to request disclosure of (i) categories of personal information collected, (ii) sources of personal information, (iii) third parties to whom the business disclosed the personal information, and (iv) what personal information was sold/shared and to whom. They may also request disclosure of specific pieces of personal information collected.
- Right to Delete: includes right to request deletion of personal information collected from the individual
- Right to Correct: includes right to request that inaccurate personal information collected by a business be corrected
- Right to Limitation: includes right to direct a business that collects sensitive personal information (as defined in the CPRA) to limit the use of such information
- Right to Opt-Out: includes right to direct a business that sells or shares (as defined in the CPRA) not to sell or share such information.

These new rights are in addition to the already-existing rights of employees under the California Labor Code to inspect and receive copies of personnel records and inspect signed documents and payroll records.

Find the Data

HR and applicant data will need to be mapped and it can "live" in many places within an organization, and not just in HR information systems or files. The use of collaboration tools like Slack and Teams increases the possibility of collected personal information that can be subject to a rights request. Once this data is mapped, it will be important to establish a process for responding to requests because you are time-limited.

Challenges

For companies that have not already established a CCPA/CPRA or GDPR compliance program, there will be many challenges to the new requirements. There are exceptions to the rights requests, but they need to be used judiciously. Employers can anticipate that such requests may be used CPRA rights may be

used as an alternative, pre-litigation discovery mechanism as has been the experience in Europe under GDPR. Emails and unstructured data will prove particularly challenging to map and inventory, particularly for companies who do not have retention policies or who have not been adhering to existing retention policies. The effective date of January 1, 2023 means that the rights under the CPRA relate to data collected as of January 1, 2022. It's time to set retention policies, especially for email, collaboration tools, and other messaging (absent a regulatory reason to retain), and ensure that the enterprise adheres to the policies.

Expanded Policies

Under the CCPA "exemptions," notices to California employees were short and sweet. Starting 1/2/23, you will be required to deliver (or make available on an intranet) a full consumer privacy notice to employees, including (a) categories of personal information collected, processing purposes, and whether personal information was sold or shared, (b) sensitive personal information collected, processing purposes, and whether the sensitive personal information was sold or shared, (c) retention period by category of personal information, (d) description of the rights available, and (e) manner in which they may exercise such rights. Regulations may amplify some of the policy disclosures, but it is not clear when those regulations will be final.

Enforcement

There is no private right of action for the failure to comply, except for security incidents arising from a failure to maintain reasonable security, which already existed under the CCPA. Under the CPRA, there will be dual enforcement by the California Attorney General and the new California Privacy Protection Agency (CPPA). And, yes, there are penalties. The CPPA has the authority to investigate violations, impose fines, and issue orders. Penalties range from $2,500 for each violation and $7,500 for each intentional violation.

Stay tuned for announcement of a webinar walking through all the new requirements for employers, and in the meantime, if you have questions, reach out to the **Mintz Privacy Team**.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.

More Viewpoints

California Privacy Rights Act Passes - Dramatically Altering the CCPA

November 6, 2020 | Blog

Read more