PERKINSCOIE

California Consumer Privacy Act (CCPA)

California Privacy Rights Act of 2020 (CPRA) vs. CCPA Compliance: Evolving Roadmap to CPRA Compliance by January 1, 2023

The CPRA qualified for the November 2020 ballot. Companies spent an estimated $5 billion to comply with the CCPA 1.0 and the California attorney general's final regulations. With the CPRA (aka CCPA 2.0) on the horizon, many companies want to know the delta between CCPA 1.0 and CCPA 2.0. This checklist is not exhaustive, and is subject to change, but provides a high-level overview of the key tasks to be undertaken between November 2020 and January 1, 2023, when the CPRA would go in effect if enacted. This resource assumes a business has mapped to both CCPA 1.0 and the related attorney general final regulations. This checklist is the delta between CCPA 1.0 and related regulations compliance and the CCPA 2.0 that must be closed by January 1, 2023. The CPRA will be subject to fresh attorney general rulemaking encompassing some 21 areas. [i]

CPRA CONSUMER RIGHTS

CONSUMER RIGHT NO. 1: GENERAL BUSINESS [CPRA 1798.100]

- ☐ **Update notice at collection**
  - Include categories of PI collected, *used, sold, or shared*
  - Include categories of Sensitive PI collected, *used, sold, or shared*
  - Develop internal policies not to use data for incompatible purposes before updating notice
  - Understand third parties will have online and offline Notice at Collection requirements if they interact on physical premises just like businesses [CPRA 1798.100(b)][ii]
- ☐ **Update contracts with vendors**
  - Prepare for obligation to enter into agreements for service providers, contractors, and third parties [CPRA 1798.100(d)]
    - Contractor agreements will be similar to the CCPA 1798.140 (w)(2) - Liability Shifted Person category
    - Third party agreements will have explicit requirements
    - Reference the Perkins Coie CPRA Vendor Checklist Chart (*available on fee basis)*
- ☐ **Develop internal policies to reflect procedures for purpose and use limitation practices** [CPRA 1798.100(e)]
- ☐ **Demonstrate reasonable security** [CPRA 1798.100(e)]
  - **Privacy Quick Tip**: We recommend a six-step program synched to a respected data security standard (e.g., NIST or ISO) and cross-reference the same to CIS Critical Security Controls[iii]
  - **Privacy Quick Tip**: Develop a memo to file documenting the reasonable security compliance, no matter the standard adopted—work with internal information security teams and outside legal counsel to prepare under privilege

CONSUMER RIGHT NO. 2: RIGHT TO KNOW PI COLLECTION [CPRA 1798.110]

- ☐ **Update privacy notices**
  - Add PI that is *shared* to privacy policy [1798.110(a)(3)]
  - **Privacy Quick Tip**: In negotiations on CPRA, some businesses indicated that they did not want to call cookie use a "sale," therefore this compromise language offered by industry was accepted
- ☐ **Update consumer rights response practices**
  - Expand to include *sharing* as defined by CPRA [CPRA 1798.140 (ah)(1)]

CONSUMER RIGHT NO. 3: RIGHT TO KNOW DATA SOLD, *SHARED*, DISCLOSED FOR BUSINESS PURPOSE [CPRA 1798.115]

- ☐ **Update privacy notices**
  - Add *shared* data to list of *sold* data [CPRA 1798.110(a)(3)]
- ☐ **Update internal policies**
  - Do not share data when consumer opts out of *sharing*
  - **Privacy Quick Tip:** Disclose cookie/tracking data that the business believes is not *sold*

CONSUMER RIGHT NO. 4: RIGHT TO OPT OUT OF SALE OR SHARING; RIGHT TO OPT-IN [CPRA 1798.120]

- ☐ **Update privacy policy to include *sharing* of PI**
- ☐ **Update web portal to include reference to *sharing of data***
- ☐ **Update opt-out to add opt out of *sharing* PI**
- ☐ **Update right to opt-in to include *sharing* of a minor's PI**

CONSUMER RIGHT NO. 5: RIGHT TO LIMIT USE AND DISCLOSURE OF SENSITIVE DATA [1798.121]

- ☐ **Create policies to respond to consumer requests to limit use of sensitive PI to the following three areas:**

California Consumer Privacy Act (CCPA)

California Privacy Rights Act of 2020 (CPRA) vs. CCPA Compliance: Evolving Roadmap to CPRA Compliance by January 1, 2023

1. To perform a business purpose as defined in 1798.140 (e)(2), (4), (5)(8) (i.e., cyber-preparedness, short-term transient use, performing services on behalf of the business, verification)
2. As authorized by future regulation under CPRA 1798.185 (c)(19)
3. A service provider or contractor can only use sensitive PI to the same extent of the business.

- If using outside of these areas, advise consumers and provide opt-outs under Section 1798.135 (a)
- If consumer limits use of sensitive PI, do not use unless the consumer consents
- A service provider or contractor may not use sensitive data after receiving instructions from the business not to use the sensitive PI and to the extent a service provider has actual knowledge that the PI is sensitive PI for any other purpose

- **Update website and mobile app links**
  - Add link to homepage to limit use of sensitive data
  - **Privacy Quick Tip:** Consider whether to combine this with Consumer Right No. 6 and have one hyperlink on the website with sub- hyperlinks
- **Update privacy policy to add right to right to request correction of inaccurate data**
- **Update consumer rights web portal to add right to limit use of sensitive PI**
- **Document any processing of sensitive data that is not used to infer characteristics about a consumer as such data is not subject to this section** [*see* 1798.185(a)(19)(C)]

CONSUMER RIGHT NO. 6: RIGHT TO DELETE [CPRA 1798.105]

- **Update internal policies to ensure the following:**
  - Once the business receives a verifiable deletion request, notify all vendors (e.g., service providers, contractors, and third parties) to delete PI [CPRA 1798.105 (c)(1)]
  - Document basis for maintaining confidential record of deletion (e.g., compliance with laws or other purposes permissible under CPRA 1798.105(c)(2))
  - Request service providers and contractors to assist the business with deletions [CPRA 1798.105(c)(3)]
- **Update internal policies for deletion requests**
  - If the business denies a deletion request based upon the need to protect security, it must demonstrate that the data is "reasonably necessary" and "proportionate" to the security threat [CPRA 1798.105(d)(2)]
- **Update website and mobile app links**
  - Do Not Sell should be updated to Do Not Sell or Share My Info
  - **Privacy Quick Tip:** Consider whether to combine this with Consumer Right No. 5 and have one hyperlink on the website with sub- hyperlinks

CONSUMER RIGHT NO. 6.1: RIGHT TO CORRECT [CPRA 1798. 106]

- **Update privacy policy to add right to request correction of inaccurate data** [CPRA 1798.106 b)]
- **Update consumer rights internal policies**
  - **Privacy Quick Tip:** Develop policies to demonstrate "commercially reasonable efforts to correct inaccurate PI," and follow policy 1798.106(c).
- **Update consumer rights web portal to add right to correct**

CONSUMER RIGHT NO. 7: RIGHT TO ACCESS [CPRA 1798.110]

- No substantive change (note that previously, the book *Implementing the CCPA: A Global Guide for Business* classified this as CPRA 1798.100(d))

CONSUMER RIGHT NO. 8: NO RETALIATION [CPRA 1798.125]

- No substantive change

NEW CATEGORIES OF DATA THAT ARE IN SCOPE AS OF JAN. 1, 2023 INCLUDE EMPOYEE AND B2B DATA.

CONTACT:

DOMINIQUE SHELTON LEIPZIG | **PARTNER**
DSheltonLeipzig@perkinscoie.com

i CPRA 1798.185
ii Different from AG Final Regs (available at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf)
iii California Data Breach Report (2016) at Executive Summary at v, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ("The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."