# IAB CPRA Toolkit

Sponsored by:

Akin Gump
STRAUSS HAUER & FELD LLP

OneTrust
PRIVACY, SECURITY & GOVERNANCE

# General Information

**The California Privacy Rights Act** (CPRA) substantially amends the California Consumer Privacy Act (CCPA) and most of those amendments become operative on January 1, 2023. Included below are practical steps that can be used in designing a company's CPRA compliance plan. The focus is primarily on changes that are needed to comply with the CPRA amendments and not existing CCPA requirements. In addition, the CPRA contemplates significant rulemaking which, once promulgated, may impact the steps identified below.

| Privacy Program Action Items (due to CPRA Amendments) | Rationale for Action Item | Operational Considerations | Resource | |
|---|---|---|---|---|
| 1. Refresh Data Map | The CPRA brings additional data sets into scope such as sensitive personal information and employee data | Enhance data mapping data model to account for categories of data such as sensitive and non-sensitive PI<br>Bring into scope systems, processes and vendors processing employee data (map where data is being processed and how to account for items such as legal holds)<br>Assess processes using automated decision making.<br>Perform discovery assessments or leverage data discovery tools to ensure full coverage of systems. | Data Mapping Questionnaire | ☐ Yes<br>☐ N/A |
| 2. Revise Service Provider Contracts | The CPRA revised the definition of Service Provider<br>Specified provisions in the CPRA are identified | Assess third-party vendors to determine where data is being transferred/processed by service providers<br>Assess where service provider addendums have been added to contracts | Vendor Addendum | ☐ Yes<br>☐ N/A |
| 3. Revise or Enter into Contractor Agreements | The CPRA provides for the definition of Contractor<br>Specified provisions in the CPRA are identified | Assess third-party vendors to determine where data is being transferred/processed by contractors<br>Assess where contractor addendums have been added to contracts | Vendor Addendum | ☐ Yes<br>☐ N/A |

| Privacy Program Action Items (due to CPRA Amendments) | Rationale for Action Item | Operational Considerations | Resource | |
|---|---|---|---|---|
| 4. Enter into Third party Agreements | The CPRA revised the definition of Third Party<br>Specified provisions in the CPRA are identified | Assess third-party to determine where they are in scope for CPRA<br>Map current contracts and agreements to determine where updates are needed<br>Update agreements appropriately | Vendor Addendum | ☐ Yes<br>☐ N/A |
| 5. Revise Data Retention Plan to:<br>• include concepts of purpose and storage limitation and data minimization and<br>• identify the time period for which each category of PI | The CPRA requires a clear statement at the point of collection regarding how long each category of PI will be retained, or, if that's not possible, the criteria used to determine retention periods. | Assess and map systems storing/processing PI to determine if retention policies are in place<br>Map existing retention mechanism (ex. internal settings for applications vs external policies)<br>Tag data fields with appropriate retention policies | Data Mapping Questionnaire | ☐ Yes<br>☐ N/A |
| 6. Disclosure of automated decision making | The CPRA requires the disclosure of meaningful information to consumers about automated decision-making technology | Assess business processes to determine where automated decision making is needed<br>Determine which systems are sourcing and storing information tied to automated decision making<br>Deploy notice on collection point sources | Data Mapping Questionnaire | ☐ Yes<br>☐ N/A |
| 7. Conduct regular risk assessments if processing of PI presents a significant risk to consumers' privacy or security. | The factors to be considered in determining when processing may result in significant risk to the security of PI shall include the size and complexity of the business and the nature and scope of processing activities. | Assess systems, processes, and vendors where PI is present to determine risk of data processing<br>Build regular assessment timelines into SOPs | | ☐ Yes<br>☐ N/A |

| Privacy Program Action Items (due to CPRA Amendments) | Rationale for Action Item | Operational Considerations | Resource | |
|---|---|---|---|---|
| 8. Conduct annual, independent cybersecurity audit if processing of PI presents a significant risk to consumers' privacy or security. | The CPRA requires a cybersecurity audit on an annual basis, including defining the scope of the audit and establishing a process to ensure that audits are thorough and independent, if processing of PI presents a significant risk to consumers' privacy or security. The factors to be considered in determining when processing may result in significant risk to the security of PI shall include the size and complexity of the business and the nature and scope of processing activities. | Perform risk assessments to determine if significant risk is posed to the consumer<br>Based on risk scoring, perform cybersecurity audit of systems holding PI | | ☐ Yes<br>☐ N/A |
| 9. Update information security policies and practices and continue implementation of "reasonable security." | A business that collects PI shall implement reasonable security procedures and practices appropriate to the nature of the PI to protect PI from unauthorized or illegal access, use, modification or disclosure in accordance with 1798.81.5.<br>Reasonable security identified in multiple contexts (e.g., third parties and verifiable requests, etc.). | Determine current set of security and risk controls and map against systems and vendors<br>Audit control implementation across business units and systems | | ☐ Yes<br>☐ N/A |
| 10. Revise Privacy Policy | Revise privacy policy to add consumer rights, additional required disclosures and obligations (e.g., add categories of SPI, right to correct inaccurate PI, consumer right not just to opt out of sale but also to "share" PI; consumer right to direct a business to limit the use of sensitive PI, make the internet website available for request to delete and correction too, etc.). | Identify currently active policies/versions and where they are displayed<br>Update policies with CPRA additions (ex. required notices and rights request methods)<br>Deploy updated notices to digital properties | Privacy Rights Guide | ☐ Yes<br>☐ N/A |

| Privacy Program Action Items (due to CPRA Amendments) | Rationale for Action Item | Operational Considerations | Resource | |
|---|---|---|---|---|
| 11. Revise Notice at Collection | Revise "Notice at Collection" to include<br>• not just categories of PI (and SPI) to be collected but also the purpose for which those categories are collected or used and whether PI and SPI is "sold" or "shared;" and<br>• the length of time the business intends to retain each category of PI, including SPI, or if that is not possible, the criteria used to determine such retention period. | Map data collection points<br>Define purpose of data collection at collection points<br>Identify where data will be transferred to a third-party and if this constitutes a share or sale<br>Ensure updated notices are deployed appropriately at data sources | | ☐ Yes<br>☐ N/A |
| 12. Revise Notice of Right to Opt-Out | Revise CCPA opt-out language to include "the right to opt-out of sale or sharing" and to limit the use of sensitive PI<br>Change the link of the internet homepage to Do Not Sell or Share My PI and add a link on the internet home page "Limit the use of my SPI"<br>**OR**<br>Include only one link if such link easily allows consumer to opt-out of sale of sharing of PI and to limit the use or disclosure of SPI<br>**OR**<br>If the business can provide an opt out through an opt out preference signal sent with the consumer's consent by a platform, technology or mechanism based on technical specifications set forth in regulations (and a business can provide a link to a webpage that enable the consumer to consent to the business ignoring the opt-out preference signal | Determine how data is being transferred to third-parties (ex. client-side vs server side, specific tech involved)<br>Determine scope of selling, sharing, and processing sensitive PI.<br>Determine how consumers are being digitally identified (ex. anonymous/device-based vs identified/authenticated)<br>Implement scripting to capture user enabled privacy signals (ex. GPC)<br>Implement technology to capture user's request and tie it to relevant technologies for request enforcement (ex. toggle on a website to disable third-party tracking technologies, a web form to capture user email and tie to downstream systems processing data) | Opt-Out of Sale/Share Guide | ☐ Yes<br>☐ N/A |

| Privacy Program Action Items (due to CPRA Amendments) | Rationale for Action Item | Operational Considerations | Resource | |
|---|---|---|---|---|
| 13. Other Suggested Internal Policies and Procedures:<br>• Mechanism to obtain opt–in consent for selling and sharing private information of minors<br>• Training Program<br>• Confidential Record of Deletion | Ensure opt-in consent is obtained for selling or sharing of personal information of minors under 16 and opt-in consent of parents/guardians is obtained for minors under 13.<br><br>Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Sections 120, 121 and 135 and how to direct consumers to exercise their rights under those sections.<br><br>The business *may* maintain a confidential record of deletion requests solely for the purpose of preventing the personal information of a consumer who has submitted a deletion request from being sold, for compliance with laws, or for other purposes solely to the extent permissible under this title. | Identity mechanisms to detect the age of minors.<br><br>Identify individuals participating in the request process (privacy, customer care, IT admins, etc)<br><br>Provide process specific training to individuals<br><br>Ensure rights requests are automatically recorded in an auditable format | | ☐ Yes<br>☐ N/A |

## Operational Changes

- ✔ Make the internet website available for request to delete and correction (not just request to know)
- ✔ Change the link of the internet homepage to Do Not Sell or Share My PI and add a link on the internet home page "Limit the use of my SPI"

**OR**

- ✔ Include only one link if such link easily allows consumer to opt-out of sale of sharing of PI and to limit the use or disclosure of SPI

**OR**

- ✔ If the business can provide an opt out through an opt out preference signal sent with the consumer's consent by a platform, technology or mechanism based on technical specifications set forth in regulations (and a business can provide a link to a webpage that enable the consumer to consent to the business ignoring the opt-out preference signal

**Interactive Advertising Bureau, Inc.** ("IAB") provides this Toolkit as a practical guide and resource for general information. Please be aware that this Toolkit does not constitute legal advice, and if you have any legal questions, please consult your attorney. While IAB has made efforts to assure the accuracy of the material in this Toolkit, it should not be treated as a basis for formulating business and legal decisions without individualized legal advice.

IAB makes no representations or warranties, express or implied, as to the completeness, correctness, or utility of the information contained in this Toolkit and assumes no liability of any kind whatsoever resulting from the use or reliance upon its contents.

© 2022 Interactive Advertising Bureau, Inc. All rights reserved. No part of this Toolkit may be sold, licensed, or otherwise commercialized without the prior written permission of IAB; provided, however, IAB hereby grants you during the full term of copyright available to the Toolkit the non-exclusive, royalty-free right and license to reproduce, customize, and use the templates, checklists, questionnaires, and guides contained herein solely in connection with your CPRA compliance efforts.