Coblentz
Patch Duffy
& Bass LLP

California Privacy Rights Act: Action Item Checklist Spring 2023 Update

California Privacy Rights Act (CPRA) gives new data privacy rights to California residents with respect to their personal information that is collected and maintained by companies doing business in California. Even if your business is compliant with current privacy laws, you must consider how the CPRA may affect your business. Below is a checklist of action items for businesses preparing for CPRA.

- Assess if your business meets new CPRA thresholds.
  - $25M in annual global revenue
  - Buy, sell, share the personal information of 100,000 consumers (California residents) annually
  - Derive 50% or more of profits from selling or sharing of personal information
- Create a personal information inventory and data flow maps to determine how, where, and what personal information is collected and maintained in your business.
- Conduct a risk assessment analysis to understand where your current practices may fall short and identify potential risks.
- Determine if your business collects sensitive personal information.
- Keep in mind data minimization principles when collecting data. Collect only what is "reasonably necessary and proportionate."
- Analyze collection, sotrage, use, and disclosure of employee data.
- Update privacy policy.
- Create a data breach response plan.
- Update your data retention policy.
- When presenting the options to opt-in or opt-out, maintain a symmetry in choice - do not make one option more difficult than the other. Do not engage in "dark patterns."
- Determine if you sell or share data as defined by the CPRA.
- Review your website(s) and see if you are using analytics. And if so, provide a notice and option for opt-out, or enable restricted data sharing settings.
- Prepare required consumer notices.
- Bolster infrastructure for handling and responding to consumer requests and documenting such efforts.
- Prepare process for verifying consumers with requests.
- Provide training for employees responding to consumer requests.
- Amend service provider agreements and update templates.
- Identify any promotions where you offer any discount(s) in exchange for personal information (like an e-mail address).
- Ensure there is a procedure in place to notify all your vendors and contractors of any requests to correct and delete the personal information of consumers.
- Analyze and implement reasonable security measures and consider applicable cybersecurity insurance.
- Monitor and audit compliance and update policies and practices as necessary or required by law.

For further information or assistance contact Scott Hall or a member of Coblentz's Data Privacy & Cybersecurity team.

Coblentz
Patch Duffy
& Bass LLP

Contacts

Scott Hall
Partner and Chair, Data Privacy & Cybersecurity Group
415.772.5798
shall@coblentzlaw.com
www.coblentzlaw.com

Mari Clifford
Associate

415.268.0504
mclifford@coblentzlaw.com
www.coblentzlaw.com

Sabrina Larson
Partner

415.268.0559
slarson@coblentzlaw.com
www.coblentzlaw.com

Amber Leong
Associate

415.268.0535
aleong@coblentzlaw.com
www.coblentzlaw.com

Bina Patel
Associate

415.268.0563
bpatel@coblentzlaw.com
www.coblentzlaw.com