Agenda

• Background
• Key Definitions
• New Consumer Rights
• New Business Obligations
• Exemptions
• Enforcement
Key Definitions

• Consumer
  o Any natural person residing in California
  o No requirement for a business or transactional relationship
  o No limitation of coverage to personal, family or household purposes
  o “Resident” means every individual who is in the State for other than a temporary or transitory purpose, and every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents. 18 CA Code of Regulations 17014.
Key Definitions

• Covered Business
  o Any for-profit legal entity that collects Consumers’ Personal Information
  o Includes entity operated for the profit or financial benefit of its shareholders or other owners
  o Determines the purpose and means of processing Personal Information
  o Does business in California
  o Either has $25 million annual gross revenue, process personal information of at least 50,000 Consumers or derives 50% of its annual revenue from selling Consumer information.
Key Definitions

• Personal Information
  - Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
  - Includes: real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers, commercial information, records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies, biometric information, electronic network activity information, geolocation data, professional or employment-related information, and inferences drawn from any of the information identified in this subdivision to create a profile about a consumer.
Key Definitions

• Collection of information
  o Buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means
  o Includes receipt from consumer directly or indirectly or by observation

• Sale of information
  o Any form of disclosure, in any format, to another covered business (or any other third party) in exchange for money or other valuable consideration
  o Excludes information provided to service providers who are not permitted to use information except to perform the contracted business service.
New Consumer Rights

• Right to request information about the business’s collection of the consumer’s personal information and to receive a portable copy of such personal information
• Right to request information pertaining to the sale or disclosure of the consumer’s personal information
• Right to request deletion of the consumer’s personal information held by the business
• Right to opt out of the business’s sale of the consumer’s personal information
• Right not to be discriminated against because of choices regarding her/his personal information
KEY CHALLENGES AND RECOMMENDATIONS

While organizations that have been focusing on General Data Protection Regulation (GDPR) compliance will be able to leverage some of that work for CCPA compliance efforts, there are still several actions required to comply with CCPA. The risk of non-compliance is significant and fines for each violation can be up to $7,500.

### Key Challenges

- **Resource Constraints**: Skillsets, availability
- **Data Requirements / Time Constraints**: 12 months’ worth of data required on effective date of January 1, 2020; data needs to be retained beginning January 1, 2019

### Key Activities

- **Create Governance Structure**: Update existing or establish new data privacy governance structure / committees to develop and implement strategy for compliance with CCPA, including potential inclusion of Chief Privacy Officer role
- **Determine Impacted Business Lines**: Identify all impacted business lines (e.g., Marketing, Sales, IT / MIS, Legal, Compliance)
- **Develop Plan**: Create high-level plan with milestones and timelines, including appropriate reporting mechanisms as well as reporting to management and the Board
- **Prepare Communication Plan**: Develop plan with endorsement from the C-suite on down throughout the company and to investors / shareholders. This will help set the “tone at the top / culture of compliance.” This should also include a reporting mechanism for employees to identify and report potential violations with the company’s CCPA program, either through supervisors or established company hotline / tip line
**KEY CHALLENGES AND RECOMMENDATIONS (Cont.)**

In order to develop and implement policies and procedures to comply with CCPA requirements, businesses should assess the current state of its data privacy program, taking care to consider all sources of covered personal information, including potential physical data records.

### Assess Current State

<table>
<thead>
<tr>
<th>Key Challenges</th>
<th>Key Activities</th>
</tr>
</thead>
</table>
| **Scope of Covered Data:** Identification of all personal data stored, sold, and shared publicly | **Assess Current State:** Identify and re-examine current data privacy policies and procedures (P&P):  
- Notifications and disclosures  
- Verifying requests  
  - Responding to requests  
    - Response time  
    - Number of requests  
- Data deletion  
- Opt-outs and opt-ins  
- Prohibition of discrimination | **Enhance Plan:** Considering the results of the current state assessment, adjust / modify plan to add more specificity to the required milestones and timelines |
| **Data / Systems Limitations:** Retention / archive capabilities, ability to identify / match consumer, ability to confirm consumer age | |
KEY CHALLENGES AND RECOMMENDATIONS (Cont.)

When addressing laws that regulate how organizations collect and use personal data, it is critical to have an understanding of what information is collected and how that proliferates both within and outside of the organization.

Key Challenges

- **Data Visibility**: Undocumented processes (Shadow IT) or unknown key processing attributes
- **Data Transfers**: Volume and speed at which data moves into, throughout, and externally from an organization

Key Activities

- **Build / Develop Data Inventory / Registry**:
  - Data will likely be contained in multiple data sources (including hard copy documents), and an inventory / registry will allow for all sources to be available for requests. Inventory of processes and key attributes:
    - Business or legal purpose for the processing
    - Individuals impacted (customers, employees, vendors, etc.)
    - Whether individuals were notified or provided consent
    - Internal systems or third parties who supply, receive, or access the data (Data Mapping)
    - Secondary uses of the data
    - Data security measures
    - Retention period
  - **Maintain the Data Inventory**: Deploy the inventory in a manner where it can continue to be updated and added to over time by the business owners. Options may include internal governance tools (e.g., SharePoint) or third party software tools
**KEY CHALLENGES AND RECOMMENDATIONS (Cont.)**

In addition to implementing and executing new processes, businesses should also incorporate these new processes into its existing risk and controls framework and related assessments.

<table>
<thead>
<tr>
<th>Key Challenges</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Develop / Update P&amp;P and Develop / Implement Processes and Controls</strong></td>
<td></td>
</tr>
<tr>
<td>➢ <strong>New Process Risks:</strong> Updated processes may lead to unforeseen risks that require identification and new controls</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>Develop / Implement Processes / Controls:</strong> Develop and implement processes, systems, and controls, including updating P&amp;P, in all applicable business units</td>
<td></td>
</tr>
<tr>
<td>• Response to verified consumer requests, including timeliness of responses</td>
<td></td>
</tr>
<tr>
<td>• Data deletion</td>
<td></td>
</tr>
<tr>
<td>• Number of verified consumer requests in 12-month period</td>
<td></td>
</tr>
<tr>
<td>• Confirmation of consumer age</td>
<td></td>
</tr>
<tr>
<td>• Length of opt-out period</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>Test Processes / Systems / Controls:</strong> Identify risks and verify that newly implemented processes / systems / controls are functioning as expected and / or identify findings / recommendations, focusing on accuracy, completeness, and timeliness of responses to consumer requests</td>
<td></td>
</tr>
<tr>
<td>➢ <strong>Conduct Ongoing Periodic Risk Assessment:</strong> Establish ongoing mechanism to identify and manage risk and to test controls, including development of monitoring and reporting to identify instances of non-compliance</td>
<td></td>
</tr>
</tbody>
</table>
KEY CHALLENGES AND RECOMMENDATIONS (Cont.)

As businesses fully implement these processes and train their staff, they should continue to track changes / updates to the regulation and incorporate into its change management process as required.

<table>
<thead>
<tr>
<th>Key Challenges</th>
<th>Key Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Identification of Appropriate Training Audience: Requirements surrounding training are broad and require training for “all individuals responsible for handling consumer inquiries about the business’s privacy practices”</td>
</tr>
<tr>
<td></td>
<td>• Develop Training Program: Create / update training programs for new processes, with a timeline for execution, including addition into annual or new employee curriculums</td>
</tr>
<tr>
<td></td>
<td>• Identify Trainers: Determine who will train impacted company personnel on the law and complying with it</td>
</tr>
<tr>
<td></td>
<td>• Hold Training Sessions: Hold workshops to train workforce on new privacy requirements, policies, procedures, processes, systems, and controls</td>
</tr>
<tr>
<td></td>
<td>• Continual Refresh: Monitor and disseminate updated trainings as required, as well as on a periodic basis, based on any changes to the regulations and / or P&amp;P updates; also promotes culture of privacy compliance through periodic and consistent employee training</td>
</tr>
<tr>
<td></td>
<td>• Enforce Standards through Disciplinary Guidelines: Publicize and enforce disciplinary actions for any identified misconduct as dictated by communicated guidelines, which will further culture of compliance</td>
</tr>
</tbody>
</table>
New Consumer Rights

• Right to request information about the business’s collection of the consumer’s personal information and to receive a portable copy of such personal information, including
  o The categories and specific pieces of the consumer’s personal information that have been collected;
  o The categories of sources from which the personal information is collected;
  o The business purpose for collecting or selling the personal information; and
  o The categories of third parties with whom the business shares the information.
KEY CONSIDERATIONS
Right to Request Information about Collection of Personal Information and Receive Portable Copy of Personal Information

- 12 months’ worth of data required on effective date of January 1, 2020
- Retention needs to begin by January 1, 2019
- All data sources should be considered, including hard copy documents

Data Requirements

Responses to Consumers

Data Sources

Number of Consumer Requests

Focus Areas

- Process and controls should be put in place to ensure that responses to consumer requests occur within 45 days
- Processes and controls should be put in place to track the number of requests by consumer (only need to respond to 2 per consumer in 12 month period)

Retention needs to begin by January 1, 2019
New Consumer Rights

- Right to request information pertaining to the sale or disclosure of the consumer’s personal information, including
  - The categories of personal information sold;
  - The categories of third parties that received the personal information; and
  - The categories of personal information that have been disclosed for a business purpose
KEY CONSIDERATIONS
Right to Request Information Pertaining to Sale / Disclosure of Personal Information

Focus Areas

Data Requirements

Responses to Consumers

Sources of Data Sold / Disclosed

Number of Consumer Requests

12 months’ worth of data required on effective date of January 1, 2020
Retention needs to begin by January 1, 2019

All sources of potential sale or disclosure of personal information must be considered and tracked, including what information provided to each party

Process and controls should be put in place to ensure that responses to consumer requests occur within 45 days

Processes and controls should be put in place to track the number of requests by consumer (only need to respond to 2 per consumer in 12 month period)
New Consumer Rights

• Right to request deletion of the consumer’s personal information held by the business

• Exceptions:
  o Information to enable solely internal uses that are reasonably aligned with the expectations of the consumer;
  o To comply with a legal obligation;
  o Where retention is necessary to complete a transaction for the individual or reasonably anticipated in the context of a business’s ongoing relationship with the consumer;
  o For security reasons such as to protect against fraudulent or illegal activity or to prosecute such activity
Segregation of Information Exempt from Deletion

Processes and controls need to be put in place to ensure service providers also delete requested information.

Historic Information

Processes and controls should be put in place to verify the appropriate deletion (and retention of exempt information) from both the business and its service providers.

Verification of Deletion

Oversight of Service Providers

Focus Areas

Personal information that is exempt from deletion requests should be clearly marked in data inventory / registry.

Data sources containing archived / historic information should be included in deletion requests, including those of service providers.
New Consumer Rights

- Right to opt out of the business’ sale of the consumer’s personal information.
  - A business may not request that a consumer who has opted out re-authorize the sale of their personal information for at least 12 months after having opted out.
Processes and controls should be put in place to determine / confirm a consumer’s age if a business does not already have this information.

Processes and controls should be put in place to confirm automatic opt-out of consumers under 16 and affirmative opt-ins.

Processes and controls should be put in place to process opt out requests, as well as to honor requests for at least 12 months before re-requesting sale / disclosure of personal information.

Personal information that is exempt from opt out requests should be clearly marked in data inventory / registry.

**Focus Areas**

- **Consumer Age Verification**
- **Exclusion of Information Exempt from Opt Out**
- **Affirmative Opt In for Consumers Under 16**
- **Honoring Opt Out Requests**
New Consumer Rights

• Right not to be discriminated against because of choices regarding her/his personal information, including:
  o Denying goods or services to such consumers;
  o Charging different prices or rates for goods or services (including through the use of discounts or other benefits or penalties) to such consumers as compared to consumers who have not exercised their rights; or
  o Providing a different level or quality of goods or services to such consumers as compared to consumers who have not exercised their rights.
Pricing policies should be evaluated to determine areas for potential discriminatory practices and updated accordingly.

If a business determines that a consumer’s data provides value that warrants a different price / level of service, it should document rationale and value provided by consumer’s data.

If a business provides financial incentives for opting in, it should document these and also ensure that these do not result in any potentially discriminatory pricing.

Complaint escalation and resolution processes should be updated to include potential discrimination allegations related to choices about personal information.

Key Considerations:
Right Not to be Discriminated Against Due to Choices About Personal Information.

Focus Areas:
- Evaluation of Pricing Policies
- Financial Incentives for Opt-In
- Value of Consumer’s Data
- Consumer Complaints
New Business Obligations

New disclosures at point of collection or in the privacy policy

- Provide at least two methods for submitting requests for disclosure (toll free phone number and website address)

- Privacy policy disclosures
  - Categories of personal information being collected, sold or disclosed during the prior 12 months,
  - Sources from which the information is collected,
  - Categories of third parties with whom the information is shared,
  - All purposes for which the information is used or a statement that personal information has not been sold or disclosed during the prior 12 months. (Additional notice is required before using for new purpose.)
  - Description of opt-out rights
  - Update privacy policy annually

- Include website home page link: “Do Not Sell My Personal Information” linking to a page enabling an opt-out.
New Business Obligations

On-demand Obligations

• Must provide 2 channels for making requests for disclosure (Toll-free telephone and webpage)
• Must respond within 45 days (can be extended for 45 more days)
• Must verify identity of requesting consumer
• Consumers may only make requests twice a year
New Business Obligations

On-Demand Obligations include responding to

- Request for disclosure of personal information collected
- Request for deletion of personal information
- Request to opt-out of sale of personal information
Practical Implications

• Review and update privacy policy
• Implement procedures for verifying requesting consumers
• Implement operations to be able to identify and locate consumer information so that disclosures can be made within 45 days
• Develop means to provide specific information disclosures electronically
• Implement Do-Not-Sell protocols for opting out (or opting-in for 13-16 year olds)
Exemptions

• Health information collected under and protected by California’s Confidentiality of Medical Information Act or HIPAA,

• Sale of information to or from a consumer reporting agency as permitted by the Fair Credit Reporting Act as amended,

• Information collected through activities taking place wholly outside of California,

• Information collected, processed, sold or disclosed pursuant to the Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act**,** or

• Information collected, processed, sold or disclosed pursuant to the Drivers Privacy Protection Act of 1994 (18 U.S.C. § 2721)**

**Exemption does not apply to private right of action for unauthorized access resulting from failure to comply with statutory duty to protect personal information.
Regulations and Enforcement

- Attorney General is required to promulgate regulations no later than July 1, 2020. (per 9/7/18 Amendment)
- Consumer rights cannot be waived.
- Violation occurs if business fails, within 30 days after being notified of noncompliance, to cure the noncompliance.
Regulations and Enforcement

• Limited private right of action for security breaches
  o May sue to recover damages between $100 and $750 or actual damages, injunctive and declaratory relief
  o Limited to actions arising from unauthorized access to unencrypted or unredacted personal information resulting from the business’ violation of its statutory duty to implement and maintain reasonable security measures to protect personal information
  o Currently required to notify AG within 30 days of filing

• General enforcement only by Attorney General
  o AG can bring enforcement actions starting 6 months after regulations are promulgated.
  o Penalties of $2500 per violation, up to $7500 for intentional violations.
For those attorneys participating, please note the following code on our attendance sheet:

CLE VERIFICATION CODE:
2018-089
Questions?