CALIFORNIA’S CONSUMER PRIVACY ACT

THREE REQUIREMENTS FOR EFFECTIVE COMPLIANCE

You can’t address risks if you don’t know they exist.
The California Consumer Privacy Act of 2018 (CCPA) removes the bar on discovery by granting California residents unprecedented access to their data held by companies. Much like the GDPR, the law reaches outside California’s law-making jurisdiction to affect a great number of organizations who hold the data of California residents ranging from consumers to an organization’s own employees.

Perhaps the greatest threat companies face under the CCPA are data access demands from residents and forthcoming litigation driven by the plaintiffs’ bar.

Unlike the GDPR, which specifically applies to information that directly or indirectly identifies the consumer, CCPA applies to any data that can be directly or indirectly associated with a consumer or household, a much broader definition of personal information.

Consequences for non-compliance are extreme—legally, financially, and reputationally. Perhaps the greatest threat companies face under the CCPA are data access demands from residents and litigation that will be driven by the plaintiffs’ bar.

**Which companies are required to comply with the CCPA?**

- For profit organizations who process the data of California consumers **AND**
- At least one of the following:
  - Annual Gross Revenues > $25M
  - Obtain personal info of >50K California consumers, households, or devices
  - Derive over half of revenue from selling CA residents’ info

**How and when should companies begin compliance efforts?**

If your organization meets the CCPA criteria, the time to begin compliance efforts is now. Enforcement for the CCPA is set to begin as early as July 1, 2020. However, there is a look-back period of one year—meaning a consumer can submit a data access request for their data held up to one year prior to the implementation date.

As Brandon Reilly of Manatt pointed out, “Companies are going to have to be compliant with most of these provisions well in advance... you need to start now”. 
It will be impossible to comply with CCPA without an accurate and up-to-date inventory of all personal data collected, stored, processed and shared – internally or with third parties. Businesses must be prepared to respond quickly and compliantly to data access requests.

Many of the rights conferred by the CCPA are new to U.S. residents. Two of the key data access rights include:

- **RIGHT TO ACCESS**: Residents have the right to request businesses to disclose the categories and specific pieces of personal information that it collects, the categories of sources from which that information is collected, the business purposes for collecting or selling the data, and third parties with whom data is shared.

- **RIGHT TO DELETION**: Residents have the right to request deletion of their personal information and require businesses to delete their data (with exemptions outlined in the CCPA).

The CCPA applies to personal data residing in all data sources and locations. Successfully navigating and responding to data access requests requires organizations to have a comprehensive understanding of where personal data exists – and it’s going to be in a lot of places, many of which will surprise you.

Unfortunately, many companies aren’t adequately prepared because they either don’t have a data inventory, or their inventory doesn’t cover all potential data sources. Simply identifying personal data held within databases fails to meet the specific and practical obligations. Visio diagrams and complex spreadsheets will not suffice.

With a comprehensive, accurate and up-to-date data inventory, companies can clearly demonstrate serious compliance efforts and respond to data access requests effectively and compliantly within the required timeframes.

As Donna Wilson of Manatt pointed out in a recent webcast on the topic, “[Data mapping is] a best practice regardless of the GDPR or the CCPA”.

### Data Inventory Checklist

- Leverage a structured profiling process with question and answer choices built around the regulation.
- Engage key business representatives across all functions and locations.
- Cover all data sources and processing activities—applications, email, shared drives, paper, and third parties.
- Incorporate data retention requirements and identify over retained personal data.
- Maintain in a centralized platform that supports routine and annual updates.

### Identify Serious Risks to Personal Data

- **Over 75%**: Of records saved in email contain personal or sensitive data.
- **Over 80%**: Of vendors processing personal data were unknown by legal.
- **Over 90%**: Of records saved to shared drives contain personal or sensitive data.

Statistics based on Data Inventories developed and maintained by Jordan Lawrence.
DISPOSE OF UNNECESSARY DATA

Any personal data that is retained, especially legacy information in email and shared drives, is available for a criminal breach, is subject to data accesses requests, and it is subject to discovery and production demands in forthcoming litigation.

Under the CCPA, companies must ensure that personal data is disposed of as soon as all business, legal and regulatory obligations for retention have been met. Out-of-date retention standards, lax enforcement, and inconsistent practices will prove costly.

A systematically enforced data retention and deletion program protects the consumer and is critical to regulatory compliance and litigation readiness. Personal data you don’t have can’t be breached and you don’t have to spend time and money producing information you don’t have.

<table>
<thead>
<tr>
<th>Data Minimization Checklist</th>
<th>Typical Data Minimization Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Develop a comprehensive data inventory and integrate proven retention standards and best practices.</td>
<td>UP TO 90% Of email can be purged</td>
</tr>
<tr>
<td>- Establish data retention standards and deletion strategies for all data sources.</td>
<td>UP TO 50% Of data on file shares can be deleted</td>
</tr>
<tr>
<td>- Issue and track preservation notices for any records and information that is subject to legal hold.</td>
<td></td>
</tr>
<tr>
<td>- Implement retention standards across all data sources including email, file shares, paper and other sources.</td>
<td>UP TO 60% Of paper records can be destroyed</td>
</tr>
<tr>
<td>- Maintain in a centralized platform that supports routine and annual updates.</td>
<td></td>
</tr>
</tbody>
</table>

Statistics based on Data Minimization programs developed and implemented by Jordan Lawrence.
California’s Consumer Privacy Act distinguishes between “service providers” and “third parties” in the following way:

- **Service providers** receive personal information from the business and process the data in accordance with the terms of a written contract with the business for business purposes (not commercial purposes). They are prohibited contractually from retaining, using, or disclosing personal information for any purpose other than to meet the terms of their contract.

- **Third parties** are any persons or entities that receive consumer information that are not 1) part of the business or 2) a service provider.

Businesses are protected in some instances when a service provider commits a violation. The same protections do not apply to third-party relationships, however. The CCPA also limits the ability of a business to disclose, sell or share personal information to third parties without providing notice and an opt-out opportunity to the consumer. This requirement does not apply to service providers, however.

To determine the level of diligence required for each of your vendors, you must first determine the access they have to your data and the level of risk they pose to your company. Most legal teams don’t have full perspective on all their third-party and service provider relationships. In fact, a recent study by the Ponemon Institute found that only 34% of respondents said they have a comprehensive inventory of all their third-parties.

Vendor risk profiling is a legal and regulatory issue. It’s not an IT problem. Effective compliance requires companies to identify service providers and third parties and have a detailed understanding of the specific types of personal data shared, processed, or managed by each vendor.
For over 30 years, Jordan Lawrence has been helping companies manage their information compliantly and defensibly. We work with many of the world’s leading organizations to ensure they effectively meet their obligations, mitigate risks, and reduce the costs of overall information compliance and control.

Legal, compliance, privacy and IT teams at companies from Avis to Wyndham rely on us to help them meet domestic and international legal and regulatory obligations for data privacy, data minimization, and third-party diligence. We leverage over three decades of deep domain knowledge, robust frameworks and standards, and a proprietary service delivery model to provide predictable, practical and defensible results for our clients.

Since 2005, Jordan Lawrence has been an Alliance Partner of the Association of Corporate Counsel. In 2018, the ACC appointed Jordan Lawrence the exclusive ACC Alliance Partner for Data Privacy and Cybersecurity Compliance.

Top law firms from around the world partner with us and leverage our services to provide clients the most comprehensive legal guidance available.

**CONTACT US FOR MORE INFORMATION:**
636.778.1700
services@jordanlawrence.com