SIX MONTH COUNTDOWN TO CCPA:

THE 10 INFORMATION GOVERNANCE STEPS NEEDED FOR COMPLIANCE

The California Consumer Privacy Act (CCPA) goes into effect on January 1, 2020. However, there is a 12 month lookback, meaning that organizations will need to be prepared to respond to consumer requests dating back to January 1, 2019.

In some ways, CCPA mirrors other privacy regulations such as the General Data Protection Regulation (GDPR), requiring the application of key privacy principles as organizations assess, design, and improve their Information Governance, Cybersecurity, and Records Management capabilities. Information Governance principles must also be considered as key components of a Data Privacy program.

BDO

10 INFORMATION GOVERNANCE STEPS TO CONSIDER FOR CCPA READINESS ACTIVITIES

1. Define Requirements

Organizations potentially subject to CCPA must understand and document their privacy requirements, understand timelines, set milestones, and assign responsibilities for executing the plan. Project management is critically important but implementing and operationalizing the CCPA plan will be an ongoing effort rather than a project with a defined start and end date. Initial considerations may include:

- Does a new program need to be designed, or is there an existing function that should own this activity?
- Who are the key stakeholders that will inform the privacy requirements?
- What does the future state need to look like?

Organizations should consider documenting legal and compliance requirements to understand the jurisdictions in which they are doing business, where customers reside, and what legal obligations are either currently in place or need to be considered. The passage of CCPA is driving other states to accelerate similar privacy regulations. As such, the US privacy landscape is ever evolving. Partnering with outside counsel, consulting organizations, and technology providers that specialize in data privacy can often accelerate CCPA readiness activities.

2. Perform Assessments

Once requirements have been defined and documented, assess your current state to determine how ready (or not) you are to meet these new regulatory obligations. A current state assessment typically focuses on the key points of the regulations to identify gaps, determine a level of maturity, and identify a roadmap to privacy compliance. For CCPA, key assessment criteria include:

- Data inventories and data flows
- Governance and operating models
- Notices and policies
- Service provider and third-party contracts
- Consumer rights processing capabilities

After a holistic assessment is conducted, privacy specific examinations such as Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs), may be advantageous to understand privacy implications at a deeper level, or for a specific company operation or technology development. Vendor assessments may also be applicable if your organization is sharing employee or customer data outside of the organization.

3. Identify Synergies

As the privacy program is developed, include stakeholders from different parts of the organization. IT, information security, legal, compliance, HR, finance, sales, marketing, and key business units commonly have a seat at the table when discussing privacy related initiatives. Understanding each function's major initiatives is critical in designing a comprehensive program to address current and future needs. By aligning each constituency, you can build out a privacy program that is not only compliant with broad frameworks like CCPA, but also addresses specific needs across the organization. For example, you may be able to align privacy activities with PCI, information security, HIPAA, or other records management initiatives already underway in the organization.

4. Identify and Address Gaps

As companies define requirements and assess their current state, potential gaps will be identified. A mitigation plan should be developed to address the gaps. Companies should clearly communicate responsibilities for addressing the gaps, including identifying and incorporating areas that may already be targeted for remediation.

5. Implement Change Management

Addressing the requirements of legislation such as CCPA can sometimes lead to potentially unsettling and disruptive changes in business processes if proper planning does not take place. Understanding your corporate culture, and employees' receptivity to change, will help determine an approach to CCPA compliance tailored to your organization.

6. Train and Create Awareness

Organizations typically deploy cybersecurity and information management training to limit exposure to data breaches due to phishing attacks and other IT security focused use cases. However, many organizations do not have data privacy related training offerings. Training should be developed, implemented, and measured to confirm that both new hires and existing personnel have not only completed the training requirements, but also understand the subject matter.

7. Communicate and Socialize the Program

Preparing for CCPA cannot be done in a vacuum. Changes to policies and related procedures will need to be clearly communicated across the organization. Companies have different mechanisms to deliver these messages. A combination of leveraging existing staff meetings, departmental update meetings, and email communications can effectively inform stakeholders of pending actions. Leveraging existing communications channels helps to make users more comfortable with any changes resulting from CCPA. If external communications are required to clients, customers, suppliers or others, those would be delivered in a similar fashion.

8. Update Documentation

Preparing for CCPA can be a catalyst to review and update company documentation. Some organizations may have recently reviewed and updated policies and procedures as part of their GDPR implementation, or in response to other regulations. Other organizations may not have reviewed or updated their policies and procedures in some time and CCPA preparations can be a vehicle to support such activities. Along with data privacy policies and updates to website privacy notices, remember to consider vendor agreements with third parties with whom you share information. Acceptable Use policies, Records Retention policies, and other technology policies such as Bring Your Own Device (BYOD) should also be reviewed to determine if any CCPA related changes are required.

9. Implement the Program

While CCPA will be effective January 1, 2020, it includes a 12 month "look back" requiring companies to catalog, preserve, and be prepared to disclose personal information dating back 12 months before CCPA's effective date. Organizations should be documenting processes now, so they have current information about how they use and share data. Organizations should also evaluate technology solutions that can help operationalize and maintain CCPA compliance programs. Also, organizations that have implemented, or are planning to implement, "Data Privacy by Design" principles can leverage these activities to accelerate CCPA readiness.

10. Monitor and Maintain the Program

While preparing for CCPA may be a focus within your organization, it should ultimately fold into more robust privacy program initiatives. With a privacy program designed and operationalized, organizations should implement an ongoing monitoring capability to identify changes and updates to the regulations and determine how best to react. As new privacy regulations are implemented, they will likely be revised and updated, so organizations need to stay vigilant to maximize program effectiveness.

SUMMARY

Debate continues in California and across the country about the CCPA. Both its opponents and supporters are still advocating for clarification and additional changes, which could mean that the regulation will be again amended before it is enacted.

In much the same way that GDPR impacted European and other international privacy programs, CCPA is a catalyst for data privacy in the United States. Organizations must start preparing now, looking to leverage similar activities that have already been initiated to accelerate their CCPA readiness. Preparing for CCPA now will undoubtedly put organizations in a better position to comply with other new US privacy regulations that are bound to be enacted soon.

CONTACT

JIM KOZIOL
Director, Records & Information Management Leader
732-734-3055 / jkoziol@bdo.com

JIM AMSLER
Channel Partnerships Director
615-493-5681 / jamsler@bdo.com

MARK ANTALIK
Managing Director, Information Governance Leader
617-378-3653 / zmantalik@bdo.com

SANGEET RAJAN
Governance & Compliance Managing Director
617-378-3653 / srajan@bdo.com

KAREN SCHULER
Principal, National Governance & Compliance Leader
703-336-1533 / kschuler@bdo.com