Globanet

GUIDE TO THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

HOW TO BUILD, IMPLEMENT, AND DEMONSTRATE CCPA COMPLIANCE

WHAT IS THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The California Consumer Privacy Act (CCPA) is a bill passed by the state of California legislature on June 28, 2018. The CCPA is set to be the toughest privacy law in the United States. It broadly expands the rights of consumers and requires companies within scope to be significantly more transpar-ent about how they collect, use, and disclose personal information. The CCPA is effective January 1, 2020, and enforcement is slated to begin no later than July 1, 2020.

The CCPA is one of the first laws to show that the US is following the current trend toward more rigorous global privacy regulations. The CCPA has many similarities to the GDPR, from its extraterritorial reach to its expansive rights for individuals, and will likely impact tens of thousands of businesses worldwide that have customers or employees located in California.
The CCPA will apply to companies if they, or an entity they control or that controls them, receive personal information from California residents, either directly or indirectly, and meet one or more of the following criteria:

- Annual revenue exceeds US $25 Million
- The entity annually receives, directly or indirectly, the personal information of 50,000 or more California residents, devices, or households
- 50% or more of its annual revenue is derived from the sale of personal information about California residents.

WHY COMPLY WITH THE CCPA?

Both the GDPR and CCPA require companies to think differently about their customers and how personal data is used. Transparency and communication about where a customer's data goes or what it's used for is necessary to doing business in the digital age. The new regulations signal a shift in expectations between customers and companies, and so companies will have to work harder to gain and keep customer trust. Companies who provide customers more control and choice over their data can build customer relationships by using that as a competitive edge.

Civil penalties under the CCPA:

California's attorney general is empowered in Section 1798.155(a) of Title 1.81.5 of the CCPA to bring an action against any company or individual person violating the Act. The CCPA allows for fines of up to $2,500 per violation or $7,500 per intentional violation, but does not place a cap on the total amount of fines. The CCPA provides businesses with a period of 30 days to remedy alleged violations of the law before a fine can actually be assessed.

For example, under the CCPA, a violation impacting 10,000 California consumers could carry a penalty of $25 million for an unintentional violation and as much as $75 million for an intentional one.

Private right of action:

The CCPA also offers a private right of action that allows consumers to seek statutory or actual damages if their sensitive personal information is subject to unauthorized access, theft or disclosure as a result of a business's failure to implement and maintain required reasonable security measures. It does not apply if the personal information is redacted or encrypted. Statutory damages can be between $100 and $750 per California resident "per incident," or actual damages, whichever is greater.

As with civil penalties, the business has 30 days to remedy the issue. If remedied, the affected consumers are precluded from seeking statutory damages, but may still seek actual damages.

HOW TO COMPLY WITH THE CCPA

The CCPA (California Consumer Privacy Act) and California A.B. 1906 (Security, Privacy of IoT Devices) were both passed soon after the GDPR, and continue the trend of California leading the US in legislating compliance standards. The EU GDPR (General Data Protection Regulation) set the stage for more choice, more transparency, and more mature privacy programs to protect personal information. Enhanced individual rights (such as access and deletion), additional transparency requirements, and required security measures are all causing companies to re-evaluate their security and data management programs from the bottom up.

Companies that have gone through a large compliance effort in the past (e.g., GDPR or ISO Certification) likely will have fewer gaps to resolve to prepare for the CCPA, but all companies in scope will have some work to do.

Before building a program, TrustArc suggests that companies review all applicable privacy compliance regulations or frameworks with which your company will have to comply. Finding commonalities between the requirements and controls will allow a company to find overlap between the obligations, and then adjust for any differences,rather than having completely separate programs.

The following chart highlights a subset of requirements that are similar for both the CCPA and GDPR. The first column provides the general area where each law has requirements that pertain to a particular subject area, forexample, data subject rights. The second column summarizes the applicable CCPA requirements, and the third column summarizes the GDPR's requirements. The last column provides a sample best practice to follow.

Privacy Requirment	CCPA Requirements	GDPR Requirements	Best Practice
Transparency	A business (controller) is under an obligation to provide consumers information such as the categories of personal information to be collected; the purposes for which the personal information will be used; and the categories of third parties with whom the business shares personal information. Include this information in the business' privacy policy and update the policy at least once every 12 months.	A controller is under an obligation to provide details such as its identity and contact details; any recipients of the personal data; and the intended purposes of processing the personal Information. Include this in a policy or notice such as a privacy notice or a GDPR-specific policy.	The compliance standard for transparency obligations is more rigorous for the GDPR, but both GDPR and CCPA require updates to your business' privacy notices/policies. Ensure your notices are updated at least annually, meet the transparency requirements of any applicable laws, and formally document that process.
Processor Obligations	Businesses (controllers) are required to convey deletion requests to their service providers. Service providers are liable for civil penalties under the CCPA. Otherwise, obligations for "processors" are much more rigorous in the GDPR.	There are detailed requirements for controllers on how to evaluate, engage, and manage processors. Processors also have obligations, and are liable for civil penalties for failure to comply.	Controllers and their processors have obligations under both the GDPR and CCPA. If your organization is a controller, ensure that you have evaluated the processors you engage and that contracts are in place with the processors. If your organization is a processor, ensure you have the requisite processes and mechanisms in place to support controllers in meeting their obligations to individuals.

Privacy Requirment	CCPA Requirements	GDPR Requirements	Best Practice
Individual Rights: Data Portability and Data Access	The CCPA provides consumers the rights of access and data portability. Consumers have the right to obtain from a business their personal information, including the categories and specific pieces of information collected; the categories of third parties with whom information is shared; and the categories of sources from which the information was. Consumers also have the right to obtain their personal information in a format that allows the consumer to transmit it to another organization. Businesses need to respond within 45 days.	The GDPR provides individuals the rights of access and data portability. Individuals have the right to receive confirmation from a controller about whether personal data about them is being processed; and, if so, additional information, including the categories of personal information concerned; the recipients or categories of recipients with whom the information have or will be shared; and the purposes of processing. Organizations need to respond within one month of receipt of the request.	The GDPR and CCPA both have the individual rights of access and data portability. Ensure that these types of requests are managed and your processes documented. Review your current process and mechanisms that are in place to respond to access requests. Assess their efficacy. Address compliance gaps and use technology tools to automate manual processes to scale and simplify.
Individual Rights: Deletion	The CCPA provides consumers the right of deletion. Consumers may request that businesses delete their personal information.	The GDPR provides individuals the right of deletion, or "the right to erasure." Organizations need to process deletion requests within one month of receipt of the request.	The GDPR and the CCPA both have deletion obligations. Review the types of data your company retains, and the legal basis for processing it. Ensure effective processes and mechanisms are in place to respond to deletion requests. Address compliance gaps and use technology tools to automate manual processes to scale and simplify.

CCPA COMPLIANCE TIMELINE

Businesses that have prepared to comply with GDPR by creating comprehensive data governance practices, records of processing, and individual rights procedures will have a head start. But, under the CCPA, all companies in scope will need to enhance their data management practices, expand their individual rights processes, and update their privacy policies by the January 1, 2020 effective date (enforcement is slated to begin no later than July 1, 2020).

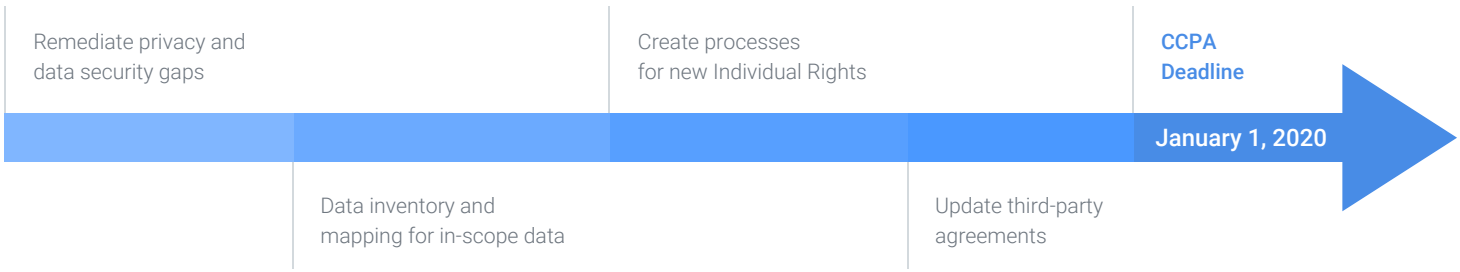
While the enforcement date is January 1, 2020, the 12-month "look back" requirement means that companies will need records of personal information collected dating back 12 months before January 1, 2020, which is January 2019. Companies should plan to create and maintain an up-to-date inventory of data processing and data flows now. While January 2020 seems far away, creating and maintaining data inventories and flows beginning January 2019 to meet the "look back" requirement will take time. With less than two months to go, companies should secure a budget, develop a process, and evaluate tools to help implement the process.

Globanet

TEN-STEP CCPA COMPLIANCE PLAN

The following ten steps provide a recommended action plan to assess CCPA compliance and build an implementation plan.

SAMPLE TIMELINE



BUILD A COMPLIANCE PLAN

1. The following ten steps provide a recommended action plan to assess CCPA compliance and build an implementation plan.
2. Conduct a gap analysis against current individual rights management policies and procedures and transparency practices.
3. Determine which business processes and activities are in scope for CCPA and which involve minors.
4. Create a data inventory of your data elements and/or update data flow maps relevant to the collection, sale, and disclosure of personal information (which are in scope).
5. Determine which CCPA individual rights apply to each business process or activity.
6. Determine whether to offer any financial incentives for the sale of personal information.

IMPLEMENT THE COMPLIANCE PLAN

1. Develop updates to individual rights management policies and procedures
2. Update Privacy Policies to include required disclosures under CCPA.
3. Update contracts with vendors and third parties with whom personal information is shared.
4. Implement individual rights mechanisms to effectively manage incoming requests from consumers.

Globanet

Globanet can help you with these efforts through our Compliance and eDiscovery solutions and proven industry expertise in the overall supervision of electronic communications. For more information, please visit us at: www.globanet.com

To learn more, contact an account executive at **888.427.5505**
or at **sales@globanet.com**