What is the CCPA?

The California Consumer Privacy Act (CCPA) of 2018 (Regulation [California] 2018/AB-3750) is an act that strengthens and unifies data protection for consumers by giving California residents more control over their personal information and how it is collected, used, and sold by companies. The CCPA was signed into law on June 28, 2018 as part of the California Civil Code and is enforced by the California attorney general. It went into effect on January 1, 2020, and enforcement will begin July 1, 2020.

Why it matters

The CCPA is the first United States law following in the footsteps of the European Union's General Data Protection Regulation (GDPR). GDPR protects EU citizens' and residents' data and privacy by outlining global privacy requirements governing how to manage and protect personal data.

The CCPA is a California-specific law, but it is far-reaching and affects any for-profit organization doing business in California. It is likely to establish a precedent for data collection and information security across the U.S. t

Data collection and protection rights under the CCPA

The CCPA gives California residents the right to:

- No more than twice a year at no-charge, request that companies disclose what personal information is being collected about them and the business purposes for collecting the data.
- Access their personal information.
- Ask companies to disclose what personal information is sold or disclosed to third parties, as well as information about those third parties
- Opt-out of the sale of personal information
- Request a business delete their personal information unless an exception applies (completing business transactions, detecting security incidences, or complying with contractual, regulatory, or legal obligations)
- Receive equal service and price and not be discriminated against for exercising their privacy rights.

Complying with the CCPA

A recent economic impact report from Berkeley Economic Advising and Research* estimates that approximately 75 percent of California businesses will need to comply with the CCPA, and the total cost of initial compliance will be $55 billion.

The truth is, managing data privacy rights, which include the right to be forgotten, right to view and understand how data is being used, and right to opt-out of processing, can be very complex and challenging to fulfill under the CCPA.

In order to meet these demands, organizations must provide a system that is scalable and flexible to address request case management, configurable workflow fulfillment processing, as well as transparency back to data subjects in a timely manner. These all are key components for organizations to be compliant with the CCPA.

How can organizations establish the policies, processes, and systems they need to comply with CCPA? ServiceNow can help.

*Berkeley Economic Advising and Research, LLC, Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations (August 2019)

CALIFORNIA CONSUMER PRIVACY ACT

Which organizations must follow the CCPA?

Any for-profit organization that does business in California and collects consumers' personal information must follow the CCPA if it satisfies at least one of the following standards:

- Generates annual gross revenue of more than $25 million
- Possesses the personal data of more than 50,000 California residents or households annually, or
- Earns over half of its annual revenue from selling the personal information of California residents

What are the civil penalties for CCPA non-compliance?

- Up to $2,500 per violation
- $7,500 per intentional violation

Highlights of the differences between GDPR and CCPA

The most significant difference?	
Basis for consent:	
GDPR consumers must **opt-in**	CCPA: consumers must **opt-out**

Other differences:	
Organizations that must comply:	
GDPR applies to any organization holding personal data on an EU citizen. CCPA applies to for-profit entities that meet specific guidelines (see above for details)	
Time allowed to respond to a request:	
GDPR: 1 month	CCPA: 45 days
Financial penalties	
GDPR: 4% of global annual income or 20m EUR (whichever is greater)	CCPA: $7,500 per intentional violation, $750 actual damage for each individual (whichever is greater)
Right to access personal information:	
GDPR: Applies to all personal data collected and processed about a subject	CCPA: Limited to data collected in the 12 months prior to a request

How ServiceNow Governance Risk and Compliance enables CCPA compliance

ServiceNow Governance, Risk, and Compliance is an ideal solution to address the CCPA. It can monitor the applications that touch personal data, provide a means to meet California resident requirements, as well as help organizations ensure that they are in following requirements when using third-party vendors.

Capabilities include:

1. Import CCPA requirements and description and policy management

   Import CCPA requirements and description

   The CCPA can be downloaded from the website: **https://oag.ca.gov/privacy/ccpa**. ServiceNow Governance, Risk, and Compliance can import all the CCPA requirements with descriptions and guidance separately or with available UCF integration. A license to import the CCPA content from the Common Controls Hub is required. ServiceNow can then map the identified CCPA requirements for an organization directly into the application, with underlying citation and controls needed for compliance checks and continuous monitoring.

   Policy management

   Organizational policies need to be aligned with the CCPA requirements for managing data protection and sharing for the last 12 months. To comply, multiple policies may need to be developed, and existing policies amended or aligned to the CCPA. Some policy examples include data protection policy, security policy, and code of conduct.

   ServiceNow offers full policy lifecycle management. Drafting a policy according to requirements through review, approval, publishing, and retirement stages are available out-of-the-box. A policy can include in the description the CCPA requirements it is designed to align with. Additionally, knowledge base policy information can be automatically created when publishing the relevant policy.

2. Data Protection Impact Assessments (DPIAs)

   Privacy compliance processes (e.g., Privacy by Design DPIA, recordkeeping) may need to be updated for California residents and households. Use DPIAs to assess processing operations that result in a high risk to Californians. Make sure to include the specific data elements explicitly listed under the CCPA as personal information including geolocation, IP address, biometric information, professional or employment-related information, education information, browsing and search history, and other noted types of data.

   Within ServiceNow Governance, Risk, and Compliance, data protection assessments can be aligned with data protection policy and underlying requirements. Although the GDPR DPIA Use Case Accelerator is named for the GDPR it can also be used for CCPA, providing the assessment templates and connectivity necessary to speed implementation of a DPIA. Additionally, all assessment requirements can be built with the Assessment Designer or enhanced with existing data protection assessments. The assessments can be scheduled on a regular basis with the outcome reflecting the compliance status of data protection.

The compliance status is reported in real time on the Policy & Compliance Management dashboard allowing for immediate remediation. Meanwhile, the controls status is automatically updated and for any non-compliant outcomes, an issue is automatically created and assigned to the responsible team member to close the requirements gap.

3. Consumer requirements

In addition to requesting information about data sharing with third parties, under the CCPA, individuals may also make access, portability and/or deletion requests. Therefore, it is important to begin tracking internal consumer and employee data flows to be able to respond to requests from consumers (e.x. CRM system, emails, HR providers, sales leads, and data agreements). A self-service portal can be very useful to providing consumers with a way to access, download and request deletion of their personal information. Service Providers should be prepared to receive similar requests from business customers.

You can utilize ServiceNow Customer Service Management (CSM) module and the Service Portal to interact with California residents and businesses (e.g., customers, staff, third parties, or contacts), providing access through its portal. The portal could include CCPA related information such as policies, procedures, and requests. It could also share data and collect requests (e.g., opt-in, access, delete information).

4. Personally Identifiable Information (PII) mapping

Protecting personal data or information requires the ability to attest to controls, assess risks, and perform audit assurance for the information assets and the systems supporting them (e.g., databases, operating systems, servers, or applications). You must be able to:

- Map information assets to other configuration items (CIs) in the Configuration Management Database (CMDB)
- Relate controls to information assets
- Relate risks to information assets
- Run audits against information assets
- Assure proper ownership of information assets

You can leverage ServiceNow CMDB to manage information assets, associate them to other CIs, and create profiles to generate risks and controls against them. A few of the capabilities to fulfill personal data asset requirements are managing risks, continuous control monitoring, and data protection impact assessments on information assets as well as on business services or on IT CIs.

5. Manage third-party CCPA compliance

Leverage DPIAs and recordkeeping to identify vendors and facilitate fulfillment of sharing disclosure requests. You should also identify third parties receiving California data and supplement and update contracts. Be aware that the CCPA requires a greater level of detail to satisfy an individual request regarding sharing of personal data than the GDPR. Therefore, you should begin tracking external data flows to understand the types of personal data (ie employee data) provided to third parties (e.g., cloud service providers, online advertisers, web analytics and benefits vendors), and whether those third parties make a commercial use of the information. If your vendors use consumer data to prioritize enhancements for their product, ask for more details–you may want to update your contract terms.

Implementing ServiceNow Vendor Risk Management provides the capabilities to ensure a vendor is meeting the requirements and protecting Californians' personal data. Specifically, Vendor Risk Management can help:

- Create a formalized tiering process
- Manage the vendor portfolio
- Design a library of assessments, based on questionnaires and evidence collection
- Schedule data privacy assessments to vendors, based on tiers or risks
- Connect questionnaire questions to GRC controls, so that the Vendors' response automatically sets the related control to compliant or non-compliant
- Deliver an external Vendor Portal for vendors to freely respond to the Privacy Assessments pushed to them.
- Manage identified issues or actions to resolution to improve the GDPR compliance of vendors

To learn more about ServiceNow Governance, Risk, and Compliance, visit www.servicenow.com/risk

servicenow