

CCPA Checklist

The California Consumer Privacy Act (CCPA) is a data privacy regulation that went into effect on January 1, 2020. Its main purpose is to protect California residents and their households by providing motivation as well as a means of enforcement to make organizations that deal with California resident information do so responsibly.

The CCPA gives consumers their data rights back, allowing them to get a complete understanding of what data is being collected, how that data is being used, and who that data is shared with.

Data Under the Scope of the CCPA

The CCPA applies regardless of where in the world you are based, but only applies if you're processing the personal information of Californian Residents, as defined in the Californian tax code, and are a for-profit business which fits the criteria.

De-identification can take data out of the scope of the CCPA. But what does it mean to de-identify data? The CCPA follows the definition used by the FTC from 2012. As defined, organizations must take reasonable measures to:

- > ensure that the data is de-identified
- > contractually prohibit downstream recipients from trying to re-identify the data.
- > publicly commit not to try to re-identify the data

Achieving Compliance

- Map & Inventory Consumer Data
 - Discover and categorize all data related to CA residents
 - Create an identity for each individual's information
 - Tag data related to CA consumers and households
 - Create and maintain data flow maps for CA consumers
 - Audit and record all third-party data sharing
- Fulfillment of Consumer Data Rights
 - Create a process for consumer data access requests
 - Identify all data that needs to be included in responses
 - Create reporting for requests
 - Validate all data rights
- Define Privacy Policies & Center of Excellence
 - Identify all applications dependent on raw datasets
 - Define a privacy center of excellence team to create data privacy policies to define how data must be transformed
 - Populate analytical systems with de-identified data that is CCPA compliant
- Validate & Test
 - Access requests
 - Data usage across business processes
 - Data lifecycle management, specifically data deletion
 - Third-party data sharing
 - Opt-out
 - Data protection policies

How Privitar Helps with the CCPA

The Privitar Data Privacy Platform™ enables organizations to build privacy into their data pipeline to meet their data privacy and protection obligations. Privitar allows companies to de-identify data in a way that retains analytical utility, powering data intelligence across the organization.

Privitar enables organizations to broaden data access in a safe way through:

- > Application of a wide variety of de-identification techniques, removing data from the scope of the CCPA
- > Protected Data Domains™ to control accessibility and linkability
- > Data Minimization of any retained data that can be tied to a consumer
- > De-identification of any data to be shared with a 3rd party

CA Consumer Rights

- > **Right to Know:** Be informed what personal data is being collected and being used in analysis
- > **Right to Opt-Out:** Choose to opt-out of having their data sold to other organizations
- > **Right to Delete:** Request that their data is deleted
- > **Right to Equal Service:** Cannot be discriminated against regardless of whether they permit sharing their data or request that it be deleted

Penalties

- > The California Attorney General can levy penalties and fines up to \$7,500 penalty for violation, and up to \$750 in civil damages per user based on privacy violations and data breach requirements
- > Individuals can file claims for privacy loss and/or compromised identities
- > Organizations must have adequate security policies and practices in place to prevent a data breach, or they could face action from private individuals

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136
US +1 857 347 4456
w: www.privitar.com



www.privitar.com