California Consumer Privacy Act (CCPA)

When the California Consumer Privacy Act (CCPA) goes into effect at the start of 2020, it is expected to be the strictest data privacy law in the United States. The new law will expand the privacy rights of California residents and includes data privacy protections and requirements similar to or broader than those imposed by the European Union's General Data Protection Regulation (GDPR) that went into effect in 2018.

What is CCPA?

CCPA affords California residents an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected.

Among other protections, the law stipulates that consumers have the right to:

- Request the deletion of personal information
- Opt out of the sale of personal information
- Access the personal information in a "readily usable format" that enables its transfer to third parties without hindrance

CCPA and Your Customer Identity Program

Principally, all California residents are protected under CCPA with respect to any information that relates to them. This means that companies around the world have to comply with CCPA if they receive personal data from California residents and if they — or their parent company or a subsidiary — exceed one of three annual thresholds:

1. Gross revenues of $25 million,
2. Obtains personal information of 50,000 or more California residents, households or devices, or
3. 50 percent or more revenue from selling California residents' personal information.

Because many forms of identity verification collect personal data including information on government-issued IDs, biometrics and/or pictures of consumers, these solutions are bound to comply with CCPA.

CCPA broadly defines personal information to cover types of information not traditionally considered personal information in the U.S., including:

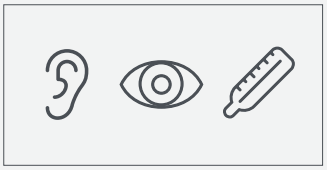
IP addresses

Email addresses

Records of purchasing or consuming histories or tendencies

Browsing history and search history

Geolocation data



Audio, visual or thermal information

Professional or employment information

Education information

What to Look for in a Compliant Identity Verification Solution

CCPA-compliant solutions should be transparent about the types of personal data collected as part of the identity verification process. Your chosen identity verification solution provider must:

- ✓ Be able to equip their business customers with a complete list of the personal data collected.
- ✓ Be able to manage consumer requests for deletion of personal data after the identity verification has been performed. If your identity verification provider stores this information on their servers, you will need a process to easily remove personal data, if requested.
- ✓ Have a policy against re-selling consumer data without prior acknowledgment (businesses should seek written confirmation that consumer data is kept strictly confidential).
- ✓ Store PII data securely and have predetermined data retention policies in place to assure the timely deletion of that data.
- ✓ Have the ability to manually override retention policies and have consumer data deleted upon written request.

Identity verification solutions that are already PCI-DSS compliant have a significant head start because of the security and data protection mandates they must meet and vet with independent auditors. Likewise, any solution that is already GDPR compliant should be able to tick most, if not all, of the compliance mandates of CCPA. Any company that is already PCI-DSS compliant has policies and third-party-tested procedures for data encryption, data retention and breach notifications. This is a far more stringent requirement than the CCPA dictates and a good housekeeping seal of approval that companies can trust — knowing the solution provider has been certified for its data protection and privacy processes.

How Jumio Can Help

Jumio enables any business that captures data from California residents with the requisite data security, transparency and retention policies to comply with CCPA.

Jumio will never sell consumer data to third parties. Just as importantly, Jumio stores and protects consumer data, captured during the identity verification process, under strict PCI-DSS data security requirements.

Jumio has the ability to delete any data captured during the online identity verification process, including information captured from the government-issued ID, biometrics and selfie images. Business customers can enforce strict data retention periods or have the identity information deleted automatically after a verification decision has been rendered.

jumio®

Learn more at jumio.com