# CCPA Compliance Data Protection Checklist

What you need to know about protecting your organization’s bottom line and consumers’ privacy.

The California Consumer Privacy Act (CCPA) gives California residents the right to know what personal information a business collects about them and request access, stop the sale/ disclosure of that data, and request that it be deleted. Further, CCPA requires organizations to implement reasonable security and protection for consumer data:

> **“Any consumer whose non-encrypted or non-redacted personal information... is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices.”**
>
> — TITLE 1.81.5. California Consumer Privacy Act of 2018

If a business doesn’t remedy CCPA violations within 30 days, it is subject to a $2,500 fine per individual whose privacy rights were violated, with intentional violations resulting in triple the fine at $7,500 per individual violation. Statutory damages can range from $100-750 per plaintiff.

## Key Terms:

### Data Subject Access Request (DSAR)

Gives individuals the right to discover what data an organization has on them, why the organization is holding that data, and which other organizations their personal information is disclosed (or sold) to.

### Personal Information

The CCPA offers a broad definition encompassing “information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

### Data Privacy Impact Assessment (DPIA)

Risk management assessment that evaluates how data processing activities may impact data subjects. While mandatory for GDPR compliance, it is optional under the CCPA.

## Data Protection Checklist

Implementing and maintaining reasonable security and privacy protections for CCPA compliance boils down to protecting California residents' private data from unauthorized access. But multi-cloud environments, continuous data sharing, and even DSARs present risks that can lead to penalties that hit your bottom line and paralyze growth.

**To minimize your risk, seek out a privacy solution that offers:**

☑ **End-to-End Encryption** — ensures only authorized users can access private data.

☑ **Access Controls** — prevent unauthorized access through controls such as disabled forwarding and revocation.

☑ **Persistent Protection** — keeps consumer data private throughout its lifecycle.

☑ **Data Loss Prevention** — automatically detects and protects private data.

☑ **Granular Audit** — supports visibility and control of private data as it's shared.

☑ **Key Management Capabilities** — host your own keys for complete control over the keys protecting sensitive data.

Together, these features protect consumer data as it's collected, processed, and shared, ensuring consumer data privacy while allowing your organization to continue developing innovative data strategies to support growth and innovation.

Virtru's persistent protection, access and discovery tools, and key management capabilities ensure no one except the requester and the organization has access to sensitive data. Applying data-centric protection guarantees that personal data stays private, no matter where it is shared.

For more information on how Virtru provides data-centric protection that prevents unauthorized access to maintain CCPA compliance, please get in touch with us to learn more.

virtru.com/contact-us

At Virtru, we understand that data is an organization's most valuable asset and sharing it is critical for business success. But sharing data creates significant risk. We believe no one should have to choose between protecting data and sharing it. We help more than 5,000 organizations, large and small, across almost every industry, protect data wherever it's created or shared so they can collaborate with confidence. Virtru provides the power to get the job done.