opentext™

eBOOK

5 things smart organizations can do to prepare for the CCPA

Now is the time to future-proof your data privacy

opentext™

Content

opentext™

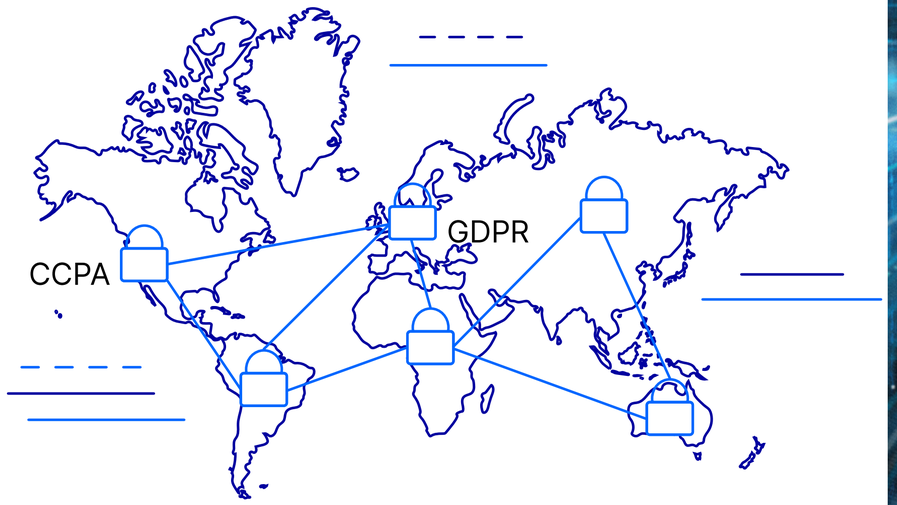
Introduction

The California Consumer Privacy Act (CCPA), which took effect January 1, 2020, is the first comprehensive United States consumer privacy law, covering the commercial use of personal data of California residents ("consumers"). Like the European Union General Data Protection Regulation (GDPR), the CCPA is expected to have a global impact given California's status as the fifth largest global economy and is considered one of the most significant legislative privacy developments in the country.

Any ***for-profit entity ("business") selling or marketing to California residents*** that meets one of the following criteria is subject to the CCPA:

- Has annual gross revenue greater than $25 million, or
- Handles personal data for 50,000 people, devices or households from California for commercial purposes per year, or
- Makes 50 percent or more of its annual revenues from selling consumers' personal information.

Building a strong privacy program requires the right combination of skills, expertise, policies, processes, training and technology tools. The to-do list can be long for organizations working to comply with data privacy laws, such as the CCPA. This eBook highlights five key initiatives to provide the best "bang for buck" to help businesses prepare for the CCPA.



opentext™

1. Conduct a data processing inventory

A business cannot comply with data privacy laws unless it knows what personal data it holds, how it is used and where it is kept. Conducting a data processing inventory, also known as a record of processing activities (ROPA) or data map, is an important first step upon which additional compliance requirements rely.

This is where to start.

What to do:

- Identify the relevant departments that process personal information, including HR, finance, legal, procurement, sales and marketing.
- Ask each Line-of-Business to identify and document the ways they process personal information. Don’t forget data managed by third-parties.
- Aggregate the entries and create a centralized master record of all processing activities.
- Document a streamlined and defensible process that can be used to keep the inventory up to date. Review and update it at least once annually.

For each processing activity it is important to ask the following questions:

- What type of data is collected?
- For what purpose is it being collected and used?
- Does the business have consent to process the data and is it documented?
- Who is the primary custodian of the data?
- Who has access to the data?
- Where is that data being stored and where does it flow?
- Is there a retention period applied to personal data?
- Are adequate safeguards in place to protect sensitive data?

opentext™

1. Conduct a data processing inventory (cont'd)

Having a comprehensive data processing inventory will:

Provide visibility into high risk areas.

Clarify the link between the data and processing purpose.

Facilitate development of records retention schedules.

Enable better and faster reporting to authorities.

Streamline subject access requests.

Examples of processing activities include:

- Employee administration
- Employee management
- Recruiting and hiring
- Vendor screening
- Contract management
- Account management
- Customer loyalty programs
- Email marketing campaigns
- Customer event invitations and registration

opentext™

2. Update and implement data retention rules

Gone are the days when companies could collect as much information about their customers as possible, use that data however they like and keep it forever.

Now, organizations must be able to clearly define (1) **the period** for which personal data will be stored, e.g., two years or (2) **the criteria to determine that period**, e.g., 20 years after a contract has expired, and implement it as policy.

What to do:

- Start with the data processing inventory. Records need to include purposes for processing, categories of personal data and the envisaged time limits for disposition of the different categories of data.
- Find a balance between too general and too detailed. Keep it simple. Not every retention period is seven years but 100 record schedules probably isn't necessary.
- Group data by (1) type of individual, e.g., job candidates, (2) data categories and (3) relevant purposes, e.g., a marketing newsletter distribution list. It is prudent to relate retention times to such groupings.
- The CCPA does not supersede existing local regulations that dictate retention periods for certain record types, for example employee and financial records.

Establishing and implementing records retention rules is not only a must-have for risk and data minimization, but it will also make life easier when it comes to subject access requests.

Examples of data categories:

- **Customer financial and tax data** is retained for the purpose of compliance with tax regulations.
- **Newsletter subscribers' information** is retained until consent is withdrawn.
- **Employee files and records** are retained for as long as required by relevant employment laws.
- **Direct marketing customer data** is retained for a specifically defined period, e.g., two years, unless the customer objects/opts out sooner.
- **Customers' contract, service or delivery data** is retained for as long as the contract is in force or services or products are provided.
- **Health records of hospital patients** are retained for the period defined by national laws.[2]

Did you know?

Only 38% of organizations have integrated privacy in their records retention policies.[1]

opentext™

3. Conduct data clean up

Most organizations store massive volumes of information in content repositories, legacy applications and email. Some of that content contains information that can identify individuals and must be evaluated for disposition. Keeping extraneous personal data can be a liability.

What to do:

- Consult the organization's records retention schedules and policy.
- Prioritize high risk systems that store the most sensitive data.
- Defensibly dispose of personal data:
  - Which the organization does not have legal basis to process.
  - Where consent of the individual has been withdrawn.
  - Where consent of the individual has expired.
  - For which approved retention periods have come up.
- Keep audit trails/records of any disposition action taken.

One of the best ways to protect personal information is to reduce the risk footprint.

A fine for poor records management

In October 2019, a GDPR fine of €14.5 million was imposed on real estate company Deutsche Wohnen SE in Germany for years of unlawful storage of old tenant data.[3] The company had used an archive system that did not include the option to delete old data and had not sufficiently distinguished between the different retention periods and partial storage obligations for the various types of tenant data. In June 2017, the Berlin Data Protection Authority issued a recommendation (warning) for the company to adjust its archive system to GDPR requirements and respect applicable retention periods. Upon a follow-up inspection in March 2019, it was determined that the company had neither cleaned up its database and could not prove a legal basis for the processing of the personal data.

This fine is highly significant as it represents enforcement taken under a data privacy law for poor records management practices and keeping too much personal information. Where the GDPR goes, other data privacy laws around the world are sure to follow.

opentext™

4. Subject Rights Requests

Perhaps the most public-facing compliance requirements for the CCPA and GDPR are the strengthened rights of consumers to understand how their personal data is being used. Meeting these requirements is important because non-compliance may result in unhappy customers and fines.

Under the CCPA, a business must be able to produce all personal information it holds about a consumer upon request **within 45 days** to comply with the:

- Right to delete personal information.
- Right to object and restrict processing.
- Right of access and to be informed.
- Right to data portability.

Responding to subject rights requests can be time- and effort-intensive. Even for organizations with mature privacy programs, challenges with information silos, legacy systems and poor search and discovery tools can make it difficult to comply with the 45-day response requirement.

For that reason, it is important to establish a step-by-step internal process or checklist that standardizes the handling of subject access requests.

Percentage of organizations that have received subject access requests by HQ location

	U.S.	EU
Access	59%	76%
Erasure	50%	72%
Rectification	22%	39%

IAPP, IAPP-EY Annual Privacy Governance Report 2019.

What to do:

- Complete the data processing inventory.
- Provide an easy way for consumers to make access requests, such as posting an email address or link on the organization's privacy notice web page.
- Establish a method to verify the identity of the consumer making the subject access request. Are they who they say they are?
- Triage requests to ensure those that are higher risk are addressed first.
- Categorize requests by status, such as new, in progress and completed, and by age. Queue management will be important for meeting the strict timelines imposed by the CCPA.
- Identify the owners of major business systems where data is managed, e.g., CRM, HR systems and shared repositories.
- Keep records of requests and their fulfillment or denial as evidence of compliance.
- Track volumes and efficiency to work to continuously improve response time.
- Configure systems to accommodate consumer requests and automate processes as much as possible.

opentext™

5. Update the privacy notice and privacy policy

The terms privacy notice and privacy policy are often used interchangeably and, although some organizations combine them, there is a difference.

A **privacy policy** is internally focused, telling employees what they may do with personal information.

A **privacy notice** is externally facing, telling customers, regulators and other stakeholders how that organization processes personal data and applies data protection principles. It is an ideal place to clearly outline how consumers can request to exercise their rights, such as the right to access, delete or have their information transferred.

Did you know?

87 percent of consumers would opt out of having their personal information sold to third parties under the CCPA rules.[4]

Under the CCPA, businesses must also include a **"Do not sell my personal information" link** in a clear and conspicuous location on a website homepage and provide an option to opt out.

CCPA vs GDPR:
Five Things to Do Now to Prepare for the Toughest US Privacy Law

Watch the on-demand webinar »

Additional resources

Explainer video—OpenText Privacy Center »

Solution overview—Prepare for GDPR Compliance with OpenText™ File Intelligence »

Blog post—Five things we've learned since GDPR »

Executive brief—Retailers: Turn GDPR compliance into a competitive advantage »

Gartner report—How to Address Data Retention and Application Retirement »

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

opentext.com

Twitter | LinkedIn | CEO Blog

Copyright © 2022 Open Text. All Rights Reserved. Trademarks owned by Open Text. For more information, visit: https://www.opentext.com/about/copyright-information (02/2022) 19485EN

Sources

1 Nymity Comprehensive Benchmark Rankings Report

2 IAPP, How to draft a GDPR-compliant retention policy, August 28, 2018.

3 TaylorWessing, First German Million-Euro Fine under GDPR Hits Real Estate Sector, November 7, 2019.

4 Adweek, 87% of Consumers Would Opt Out of Ad Targeting Under CCPA Terms, October 2, 2019.