PKWARE

pkware.com

CCPA Overview

Sensitive and Personal Data Protection Requires Privacy Operations

2021

Contents

The Need for Privacy Regulations

It is personal data that traces and reveals our essence—personal data represents the footprints of our lives. People naturally want some control over who has access to or use of their personal data. Explosive growth in technology provides people a constant stream of choices of whether and when to connect and share their personal data. Artificial intelligence and machine learning enable companies to collect, track, and sell vast amounts of personal data about people's connections, choices, and day to day activities.

Technology tipped the scales heavily in favor of entities' limitless sharing and uninvited access to people's sensitive information—and privacy data regulations have been emerging in response to people's legitimate concerns.

Privacy regulations give people a chance to exercise their privacy rights. These regulations try to be broad enough to fit a wide array of types and sizes of businesses,

The CCPA applies to companies that do business in California and:

- Have annual gross revenue in excess of $25 million
- Annually buy, receive for commercial purposes, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices.

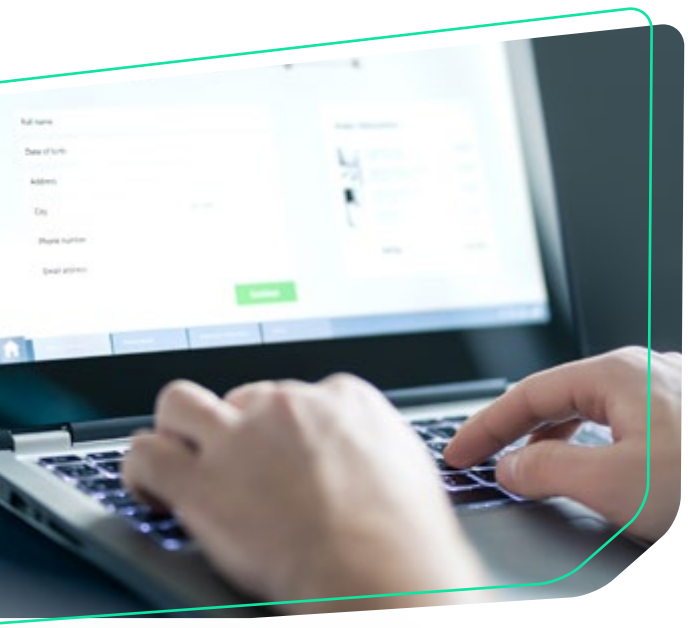
- Derive 50% or more of its annual revenues from selling consumers' personal data

The regulations cover collection, use, processing, sharing, and selling personal data of customers, employees, or other individuals.

while following the life cycle of personal data from collection to disposal. Regulations commonly include rights, jurisdictions, timelines for requirements, and the various costs of non-compliance. Companies then develop internal data privacy policies and procedures to operationalize the regulations for their unique environment and needs.

PKWARE: Integrated Discovery, Classification and Protection

The CCPA requires companies to have a "Do Not Sell My Info" link on websites, giving consumers the right to opt out from those companies selling and disclosing their personal and sensitive data. The opt out only stops the selling of personal information There is no impact other uses of their information.



The CCPA's definition of "sale" applies to an exchange for value with third parties of people's personal information, including data that cookies or other technologies capture. Companies' methods for submitting requests to opt out have to be easy for consumers to execute and use minimal steps to allow the consumer to opt out. A business may not design a method intentionally to or having the substantial effect to subvert or impair a consumer's decision to opt out.

Businesses must comply with an opt-out request within 15 business days.

Companies must comply with Data Subject Access Requests (DSAR) with Right to Know and Right to Be Forgotten reports and compliance within 45 business days. There are only a few exceptions when a company would not have to comply with a DSAR, including when the identity of the requestor cannot be verified, or in the case of personal information of a child under 13 when the identity of the requestor as parent or guardian cannot be verified.

Penalties

Penalties for non-compliance range from $2,500 for an unintentional violation to $7,500 for an intentional violation. Children's personal data violations are subject to the same fines as violations involving adults. A company is not considered liable if it cures any noncompliance within 30 days after being notified of alleged noncompliance. Individuals can bring a private complaint or right of action only if there is a breach of unencrypted and unredacted sensitive or personal data.

Critical Technology Gaps

Understanding the technology gaps your company has is important for prioritizing activities, budgeting, and gathering resources. There are several critical technology gaps that impact the ability of companies across sectors and jurisdictions to comply with privacy regulations.

Scanning All Data Stores, Servers, Endpoint Folders, and Files

Your company's retention and use of personal data are ethically and legally limited. The CCPA limits your organization's sharing or selling personal data to other organizations.

To manage personal data your company has, first discover the location of all of it. Find out when and with what third parties your company has already shared data. You may be legally audited by regulators and are responsible for a breach by your own company's and your third parties' handling of your personal information.

Discovering sensitive data and personal data across your entire platform is not easy. Some personal data your organization collected directly. Other personal information you may have sourced third-party. Some you may have shared across your organization while growing your services and relationships with customers, or perhaps you shared some personal information with solution partners or other third parties.

As an example, labeling headers and formatting the same types of information in tables or other files can typically be inconsistent across various departments and when coming from external sources, some may use words or labels that you can't readily make sense of. Thus, traditional database searches to find sensitive data fail.

While personal information may sometimes be discovered in structured data, it also sits in unstructured and semi-structured data. That makes its identification and location more difficult, time-consuming, and prone to errors and omissions.

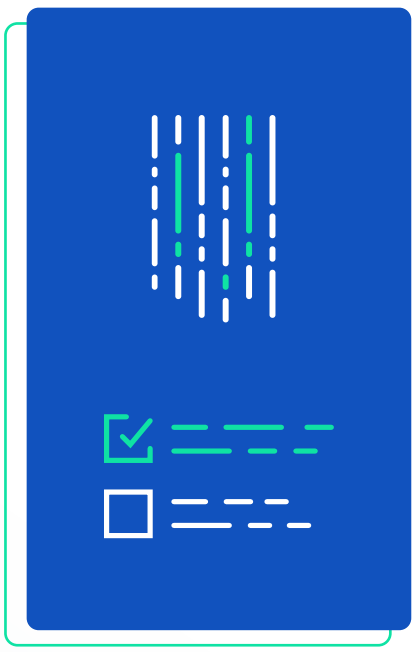
Personal data sits in an array of your distributed databases, and other data stores, whether on-premises or in the cloud managed by cloud platform companies—think Azure, AWS or Google—or some hybrid. It also sits in your laptops, desktops, devices, and folders and files being shared or copied who knows how often in conducting normal business.

Use Technology and Operational ReadinessTogether

The CCPA requirements are best met by following strategic, targeted operational processes (privacy operations) and technological processes (privacy engineering) in tandem.

Operationally, socialize your data governance policies thoroughly and make them known throughout the organization. Encourage and internalize company culture of privacy protection as a matter of commitment to the protection of human rights; externalize and market your commitment strategically and clearly. Be proactive in keeping personal information you receive from third parties to a minimum and track when and where you share personal information under your policies.

Technologically, conduct thorough, scheduled scans of your data to consistently know both the source location as well as timing of sharing, receiving, or using any personal data. Develop the capacity to inventory and catalog your personal information to meet requirements of the CCPA.



Identifying data elements—including particular categories of data elements—is challenging. As an example, CCPA has a specific requirement in discovering data used for making inferences about a person.

Companies need technical, smart methods to make sense of structured, unstructured, and semi-structured data and correctly identify which contain sensitive and personal data.

Another complex area to solve is recognizing data types, both at rest and in motion, as they are entering and leaving your organization, then connecting all the sources and destinations to that personal data and indexing it all. Using advanced technology methods such as sampling, probability, and machine learning helps you accurately discover all your sensitive data and personal information.

Creating Reliable Identities

Discovering the specific persons or data subjects impacted by the regulation and knowing which sum of all the vast personal data is for what person, and then creating a comprehensive, reliable identity, is not simple. Being able to associate different data elements with a person correctly is the first step. Then you'll need the ability to match that same person across different systems and distinguish who is who among other people. Even the names of people can present a challenge in data being mistakenly associated.

Protecting Sensitive and Personal Data

Having discovered all the personal data and correctly created and built full identities, now you are required by the CCPA to protect all the personal information. How do you do that? You establish sensitive data policies.

Companies continuously acquire and use petabytes of data filled with sensitive, personal information that has to be protected. The first goal is to reduce the use and storage of personal informational elements to the minimum needed. Retaining unnecessary personal data increases your organization's risk of liability. Choose world class technology that scales with your data volumes to regularly scan, locate, and eliminate all unnecessary and unneeded personal data to reduce your organization's risk of exposure.

All companies have orphaned identities they are not aware of sitting amidst their data. Orphaned identities are those of individuals that cannot be tied to any processing activity and so, essentially, any privacy commitment. The ability to discover your orphaned identities and eliminate them is challenging, but saves overhead cost and possible embarrassment.

Other key techniques for protecting sensitive data in adhering to the CCPA are format-preserving masking, redaction, and encryption. The right solutions protect the individual's identity and still preserve the data's business value to your company for test and analytics purposes. Choose technologies that are sophisticated—with an adaptable, intelligent architecture—to confidently make sense of sensitive data elements and their true meanings and purpose at scale, then implement policies that apply the right protection techniques across the board while maintaining your competitive posture in the market.

Responding to DSARs

Where the rubber hits the road is in being ready and able to accurately respond to DSARs received and send out timely reports.

The Right to Know and the Right to Be Forgotten are protected rights. A DSAR is the mechanism any individual can use to find out what personal information your company has about them, when and how it's been used, and then decide whether that is all okay or if they want you to delete it all. The spotlight is on your company. You've got to be well prepared, accurate, and fast to assemble the required reports for the verified requestor.

Automating your DSAR intakes and responses will save your company countless hours while delivering the accuracy and efficiency required by the CCPA. Your organization then has to be able to securely communicate the data in the reports first internally and then with the verified requestor. You have to assign technical and operational responsibilities by roles across your organization, set up an internal review process, and build uniform, accurate responses.

PK Protect Platform Provides You the Capabilities to Handle What the CCPA Requires

- Scan all files, systems, and repositories that contain personal data and contextualize sensitive privacy information with PKWARE AI-infused software
- Create and maintain inventories of personal data and robust, unique identities of all individuals

- Apply appropriate privacy policies to meet the CCPA requirements from over 100 out of the box options without a single line of code
- Respond fully and on time to Data Subject Access Requests (DSARs) with individualized reports, based on PK Discovery identity creation and company-defined privacy policy application.
- Scan all files, systems, and repositories that contain personal data and contextualize sensitive privacy information with PKWARE AI-infused software
- Create and maintain inventories of personal data and robust, unique identities of all individuals

Apply appropriate privacy policies to meet the CCPA requirements from over 100 out of the box options without a single line of code

Respond fully and on time to Data Subject Access Requests (DSARs) with individualized reports, based on PK Discovery identity creation and company-defined privacy policy application.

About PKWARE

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance. To learn more, visit PKWARE.com.

Enterprise-Wide Policy Management

PK Protect provides a point of control for data protection activity across the entire organization

Simple Workflow

With PKWARE, data protection is automated for end users and easy for administrators to manage

Easy Implementation

PKWARE supports a variety of deployment options, enabling organizations to implement their data protection solution without time-consuming changes to infrastructure and workflows

Protection Without Gaps

PKWARE works on every enterprise operations system and provides persistent protection that remains with data even if it's copied or shared outside organizations

Integrated Discovery, Classification and Protection

No other solution has the capability to find, classify, and protect data in a single automated workflow

Multiple Protection and Remediation Options

Organizations can take a policy-based approach to data protection and choose from action including persistent encryption, quarantine, masking, and deletion.

BOOK A DEMO

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance.
To learn more, visit PKWARE.com.

PKWARE

PKWARE.com

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204