Lepide

Datasheet

California Consumer Privacy Act (CCPA)

About CCPA

The CCPA has three main objectives to improve how the personal information of consumers is handled by organizations. The first objective is to provide consumers with the awareness of the type of information that enterprises are collecting. The second is to provide more rights to consumers about how their information is shared or sold with third parties. And the third is to provide added protection to consumers against enterprises that are not taking privacy and security seriously.

Who the CCPA Applies To

Businesses that must comply with the CCPA are any entity doing business in California operating for the profit or financial benefit of its shareholders that collects the personal information of consumers. Businesses that meet these criteria must also meet at least one of the following thresholds to qualify for CCPA compliance:

1. Annual gross revenue of over $25 million
2. Collects (buys, receives or sells) the personal information of 50,000 or more consumers, households or devices on an annual basis
3. Gets 50% or more of its annual revenues through the selling of consumer personal information

There are a few key exemptions from the CCPA. Notably, if you are a healthcare provider already covered by HIPAA or a financial services provider covered by Gramm-Leach-Billey.

A Few Key Definitions

Compliance regulations in general can tend to be vague when it comes to defining specific terms used, and the CCPA is no different. We've already defined who the CCPA considers to be a covered entity – and that definition appears to be straightforward.

The definition of a consumer, however, is slightly vaguer and worth making a note of. It is defined as any person residing in the State of California. A resident is defined as either someone who is in the state for more than just a temporary or transitory period, or an individual who lives in the state but is outside of the state for a temporary or transitory period.

Similarly, the definition of personal information is generously vague (as is the case with a large number of compliance regulations). In general, personal information is data that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device." In other compliance regulations, this kind of data is often referred to as personally identifiable information (or PII).

The CCPA does provide a list of examples of data that falls under this definition, including names, addresses, property records, biometric data, browsing history, passport numbers etc. If you want to be safe, you should assume that any information you collect on an individual should be considered personal information and kept appropriately secure and private.

Consumer Rights Under CCPA

As we previously mentioned, the CCPA aims to give consumers greater insight and control over how their personal information is collected, stored, processed and shared. This is achieved through the implementation of four specific consumer rights.

Right to Access: California consumers will be able to formally request that covered entities disclose to them exactly what information has been collected, where it has been collected from, why it has been collected, who it will be shared with and more.

Right to Opt-Out: If a California consumer does not want a covered entity to sell or share their personal information, they have the right to opt-out – effectively preventing that covered entity from doing so.

Right to Deletion: California consumers have the right to request that covered entities delete the personal information that they have collected should they wish to have it deleted.

Right to Equal Service and Price: This is a caveat that protects California consumers from being discriminated against should they exercise the rights of the CCPA. Essentially, covered entities cannot deny goods and services to consumers that have exercising their rights under the law.

Control Description - §1798.150 (a)

(1) Any consumer whose nonencrypted or nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

Control Processes

Identification and Authentication
Access Control
Configuration Management
Incident Response
Risk Assessment
System and Information Integrity

Control Processes Facilitated by Lepide

To address this broad provision, an organization needs to implement a wide set of security procedures and organizational improvements from several different control families; no particular control process alone can ensure compliance with this requirement.

Identification and Authentication

The objective of this control process is to ensure that all users and devices are uniquely identifiable and verifiably authentic before they are granted access.

User Identification: Use our state in time reports to determine which user accounts have access to the systems. Cross reference this with HR to determine the business need for each account. Identify accounts that cannot be linked to real people.
Use our user behavior analytics engine to audit the use of shared accounts and ensure they are being used appropriately.
Spot suspicious user activity in relation to employee absences by cross-checking HR data with logon activity reports.

Device Identification: Use our state in time reports to cross-check IT inventory against computer accounts. Use our change reports to spot any unauthorized changes to computer accounts.

Identifier Management: Use our change repots and our interactive search to identify unauthorized creation, modification or deletion of users and groups. Use our real time alerts to configure alerts for unauthorized changes.

Authenticator Management: Use our change reports to spot unauthorized changes to account policy, password policy, and GPO link changes. Set alerts for Group Policy changes related to account passwords. Run reports on password resets.

Access Control

The goal of this is to ensure that users are only being given access to the data they need to do their job.

Account Management Audit: Audit changes to user accounts, detect recently created user accounts, and more with predefined reports.
Set alerts to be sent to designated personnel at the detection of any unauthorized changes.

Account Usage Monitoring: Review user access to sensitive behavior with proactive monitoring and receive real time alerts when user behavior is deemed to be anomalous. Real time alerts and automated threat response enable security teams to respond to threats promptly.

Inactive Accounts: Easily identify inactive accounts with a pre-defined report.

Role and Group Assignment: Identify any security group membership changes with pre-defined reports.

Personnel Status Changes: Review detailed audit trails to confirm that temporary and ex-employees are disabled or can no longer access sensitive data.

Access Enforcement: Run pre-defined reports to determine users with excessive permissions.
Govern access from within the solution.
Determine how permissions are being granted and revoke where necessary.
Real time alerts and threshold reports for changes to permissions.

Least Privilege: As above. Any changes to permissions, configuration and anything else that would affect access to data, can be reported on.

Audit and Accountability

The objective of this section is to ensure that you keep an audit trail that can be used to investigate incidents and hold individuals accountable for their actions. Lepide keeps an audit trail available for more than a decade to help you do exactly that.

Produce hundreds of audit reports for all states and changes that are being made to both infrastructure and sensitive data.

Incident Response

The objective of this section is to ensure that you have a way to identify and react to incidents quickly and efficiently.

Incident Detection: Real time alerts for unauthorized changes, anomaly spotting and risk analysis reports help you detect potential incidents.

Incident Analysis: Our interactive search and easy-to-read audit trail of events make investigations and analysis easy.

Incident Mitigation: Run automation threat response models on the detection of unwanted events to locate and mitigate the threat in real time. Restore unwanted changes and deleted objects easily.

Risk Assessment: Use our risk assessment dashboard to identify any potential risks to data security, including excessive permissions and over-exposed data.

System and Information Integrity

The point of this section is to protect information and systems from being compromised by both external and internal threats.

Information System Monitoring: Spot anomalous user behavior in real time get alerted on any potential malicious activity/changes.

Information Management and Retention: Identify PII and other protected/sensitive data and ensure the appropriate access controls are applied by seeing who can access/modify it. Simplify subject access requests.