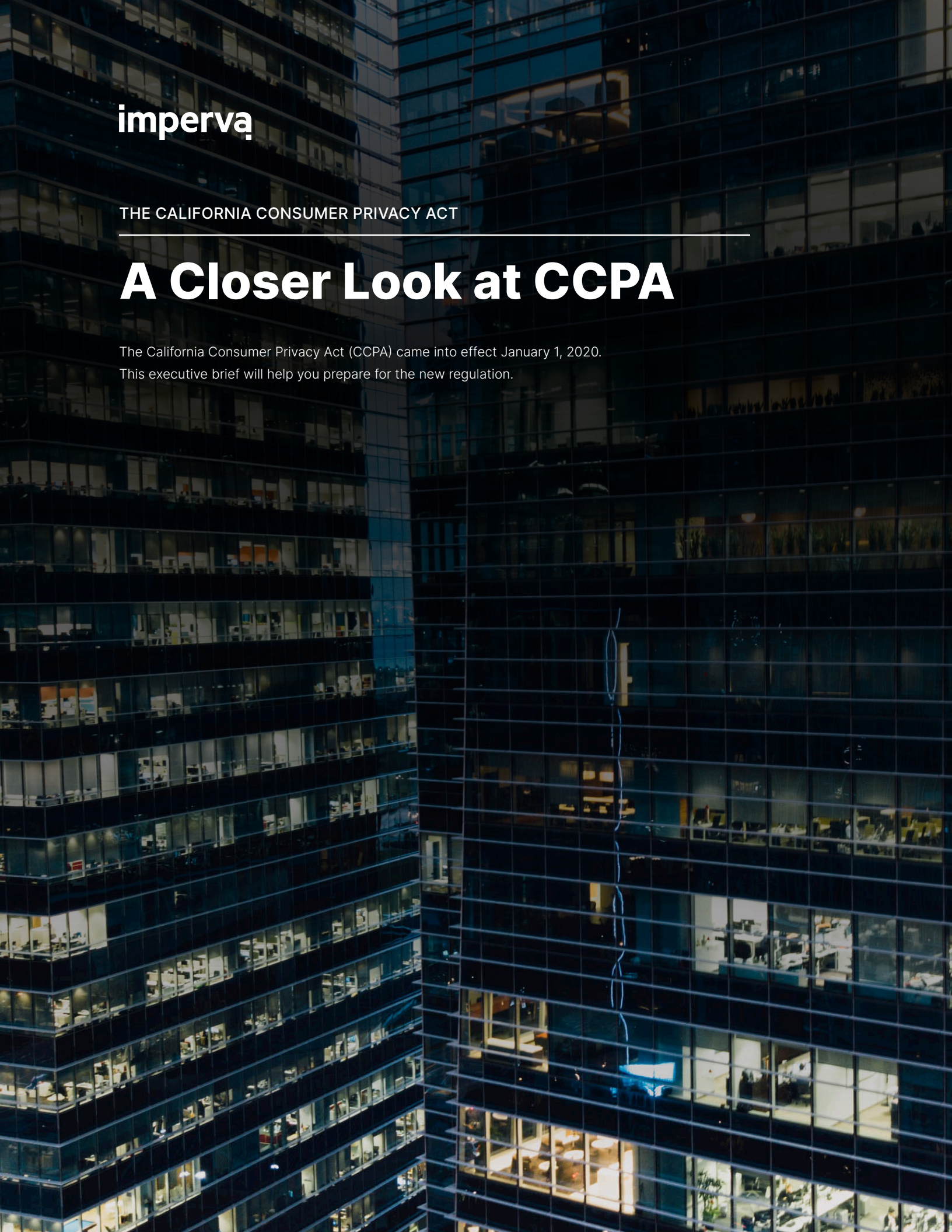

imperva

THE CALIFORNIA CONSUMER PRIVACY ACT

A Closer Look at CCPA

The California Consumer Privacy Act (CCPA) came into effect January 1, 2020. This executive brief will help you prepare for the new regulation.

Contents

What is the CCPA?

The California Consumer Privacy Act (CCPA), passed in 2018, is meant to improve privacy rights and consumer protection for residents of California. The new act draws much from Europe's General Data Protection Regulation (GDPR) as it relates to the access to, deletion of, and sharing of personal information. Its intent is to provide Californian citizens with the right to know when their personal data is being collected, whether their personal data is being disclosed or sold, and to whom.

The act also intends to provide consumers with the right to:

- Say no to the sale of personal data
- Access their personal data
- Request that a business delete their personal information
- Not be discriminated against for exercising their privacy rights

When did it come into effect?

The legislation came into effect on January 1, 2020 with regulatory enforcement expected to begin six months later on July 1.

SECTIONS OF THE CCPA

Who needs to comply?

The CCPA applies to any business that collects the personal data of consumers based in California and that meets any one of the following thresholds:

- Has annual gross revenues in excess of $25 million
- Possesses the personal information of 50,000 or more consumers, households, or devices
- Earns more than half of its annual revenue from selling consumers' personal information

All businesses that collect the personal data of California residents and meet the above thresholds must comply with the CCPA, even those that have no physical presence in Californian and are not otherwise ruled by California law.

If you are a California citizen who temporarily resides outside the state, you are still protected by the CCPA.

Definition of personal information

Under CCPA, personal information is defined as any information that could be reasonably linked to a particular consumer or household, including a real name, alias, postal address, unique personal identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

Violation or data breach

The CCPA could have significant implications for litigation including injunctive, declarative, equitable relief and data breach litigation. Violation of the CCPA regulation or a data breach can result in the following penalties:

- Organizations that become victims of a data security breach can be ordered in civil, class action lawsuits to pay statutory damages of between $100 to $750 per California resident and incident, or actual damages, whichever is greater.
- A fine up to $7,500 for each intentional violation and $2,500 for each unintentional violation.

Agility, data privacy, and security

One of the key findings of the California state legislature is that as the role of technology and data in the daily lives of consumers increases, so too does the amount of personal information they share with organizations. This data growth and the simultaneous increase in cyberattacks and data breaches is making data security a top priority for businesses around the world and driving more stringent data privacy regulations.

More digital interaction with data means companies find themselves having to store growing volumes of personal customer data. This makes data security and regulatory compliance more of a challenge. To fully protect their assets and meet data privacy requirements, businesses need to know exactly what data they possess, where it is stored, and who has access to it.

The CCPA requires businesses to create a number of new procedures to meet requirements including:

- Respond to requests from consumers who want to see the personal data that the company has stored, delete their personal data, or ask a company not to sell their personal data.
- Verify the identity of consumers who make such requests.
- Disclose financial incentives offered in exchange for the retention or sale of a consumer's personal information.
- Maintain records of requests and how the business responded for 24 months.

CCPA and GDPR differences

The CCPA is often compared to Europe's General Data Protection Act (GDPR) and it's fair to say that organizations that have ramped up to GDPR compliance will find it easier to meet the requirements of CCPA. Businesses should not assume, however, that complying with GDPR lets them off the hook. While there are similarities – for example both regulations give individuals the right to access and delete their personal information - they are two separate legal frameworks and that impose different obligations.

Some differences:

- The CCPA definition of personal information specifically includes household information whereas the GDPR definition of personal data applies only to any information related to an identifiable natural person.
- The content in the required privacy notices differs for each of the regulations and a privacy policy that meets the requirements of the GDPR will likely not satisfy the CCPA privacy requirements, which must include how to restrict the sale of personal information.
- Under the CCPA, individuals have the right to opt-out of the sale of their personal information and organizations are obliged to add a "do not sell my personal information" button to their websites which is not a requirement of GDPR.

To provide true data privacy for consumers and to implement any of the above procedures for CCPA compliance, organizations need to fully understand what personal consumer information they have stored on their networks, who has access to it, and how to protect it. Large organizations that store high volumes of data will find this especially challenging as they often manage multiple locations and store data across multiple environments. Their data security teams can receive tens of thousands of threat alerts daily causing alert fatigue and the risk of a serious threat slipping through the net.

How Imperva can help

To help organizations comply with CCPA obligations, the table below cites the relevant sections of the regulation aligned with the respective Imperva solution.

Imperva offers a range of data security solutions that help organizations meet data privacy and protection compliance obligations.

Data discovery and classification

Where is personal data stored?
CCPA Sections: (1798.100, 1798.110, 1798.115, 1798.120, 4798.105)

The Imperva Data Discovery and Classification solution scans your network and servers to find any unknown databases, pinpoints and classifies sensitive data using dictionary and pattern-matching methods, and can scan database content for pre-defined data types such as credit card numbers, national identifiers, email addresses, system credentials, and more. This helps companies take a risk-based approach to their data security by evaluating and prioritizing which datasets require which levels of protection to reduce the impact of a breach and reduce risk to their organization.

Data monitoring

Which data has been added or updated within the last 12 months?
CCPA Sections: (1798.100, 1798.130)

Imperva Data Security solutions provide enterprise-wide visibility into all database activity by monitoring all user database access, on-premises or in the cloud, and retains all the audit logs.

Using policies that Imperva provides for regulations such as CCPA, organizations can identify the user by role (including privileged users) or account type (such as a service account), know whether the data accessed was sensitive, and easily detect non-compliant access behaviors. This automates detection of the nature or origin of a threat and helps to accelerate any required incident response. Organizations can create custom policies of their own as needed.

The policies also allow an organization, at their discretion, to automate breach prevention responses such as terminating the download of a large number of sensitive database records.

Data risk analytics/RASP/WAF

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.
CCPA Section: (1798.150)

Imperva Data Risk Analytics (DRA) uses machine learning to automatically uncover unusual data activity, surfacing actual threats before they become breaches. DRA provides granular visibility and actionable insights into how data is being used and by whom so that companies can quickly detect unusual behavior, enabling them to contain a breach before damage happens.

Imperva's Runtime Application Self-Protection (RASP) detects and blocks attacks from inside the application. RASP monitors all traffic through your applications showing you which vulnerabilities in your applications are under attack, who's attacking and how, and what they're trying to accomplish. The result? Fast and accurate protection with NO signatures and NO learning mode.

Imperva WAF works on-premise and in the cloud, to protect against the most critical web application security risks accurately detecting attacks and minimizing false positives. Through an intuitive single pane of glass dashboard Imperva WAF enables you to quickly assess security status and streamline demonstration of regulatory compliance.

Data masking

"Pseudonymize" or "pseudonymization".
CCPA Section: (1798.140)

Imperva Data Masking protects sensitive data from exposure in non-production or DevOps environments by replacing sensitive data with fictional but realistic values using a variety of masking techniques including pre-defined or customer data transformers. Data masking reduces the risk of sensitive data exposure, prevents data security breaches, and helps you comply with data protection and privacy laws.

Conclusion

Digital transformation has made more and more data available everywhere resulting in unprecedented levels of data availability and accessibility. With regulators stepping up to enforce tighter data protection laws, data security and data-driven compliance have become two major priorities for companies in recent years. As California will be the first state to pass anything similar to the GDPR in the United States, CCPA could be the tip of the data privacy regulation iceberg.

Find out more about Imperva Data Security and compliance solutions here.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.