XTIVIA

www.xtivia.com
888-685-3101 ext. 2

GUIDE TO CCPA

The following information outlines the regulations, standards, and important facts about the California Consumer Privacy Act (CCPA).

New Consumer Privacy Rights Under CCPA

Under California Civil Code § 1798.83, the rights for Californians are as such:

- The right of Californians to know what personal information is being collected about them
- The right of Californians to know if personal information about them was being sold or disclosed and to whom
- The right of Californians to say, "no" to the sale of personal information
- The right of Californians to access their personal information
- The right of Californians to equal service and price even if they exercise their privacy rights

The right to be forgotten:

- Similar to the General Data Protection Regulation (GDPR), under CCPA, consumers can request to have their information erased, and companies must comply.

CCPA Objectives

- Data Control: Consumers should control who gets access to their personal data/information.
- Data Transparency: Companies should be transparent about what data they collect and how they use it.
- Data Accountability: If companies misuse consumer data, they should be held responsible.

Who Does CCPA Apply to?	
✓	Your company does business in the state of California
	AND
✓	Your company does $25M+ in annual revenue
✓	Your company collects data from 50K+ individuals a year
✓	Your company makes half its revenue via selling personal data

Actions Moving Forward

Provide Clear Disclosure: On any page of your site where visitor data is being collected, you need to provide full disclosure of the following:

- Their rights are under the CCPA
- The type/category of data being collected
- How collected data will be used (including if it will be shared and to whom)

www.xtivia.com
888-685-3101 ext. 2

Consumer Request Processes: Companies need to outline the processes and protocols to deal with consumer requests, including:

- Requests to view all data the company has collected about them
- Requests to delete all data the company has about them (from the last 12 months)
- Requests to opt-out of the selling of collected data

Penalties

Noncompliance

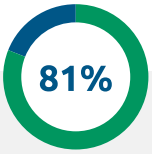
- **$2500** per unintentional violation
- **$7500** per intentional violation

Data Exposure via Breach/Hack

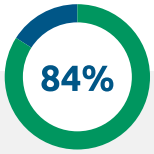
- Consumers can sue a company for **$100-$750** per incident (if damages exceed **$750**, they can sue for more)

Secondary Effects of GDPR Compliance | What could be seen with CCPA Compliance

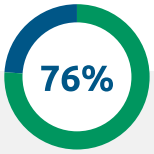
A 2019 report by the Capgemini Research Institute



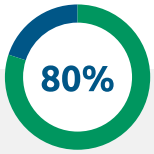
said GDPR had a positive impact on the organization's reputation/brand image, which helped with leads for marketing.



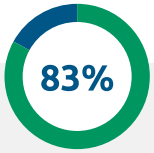
saw an increase in trust among their customers.



saw increased revenue and improved customer loyalty and online purchasing.



agree that the number of data subjects targeted in campaigns has increased.



of compliant businesses saw an increase in online purchases.

Based on the Capgemini Research Institute report, "Championing Data Protection and Privacy**."*

The major differences between CCPA and GDPR.

Range of Protection

CCPA

Protects the data of C.A. residents. Any company doing business in C.A., and (a) makes $25 million gross revenue annually, (b) collects data from 50K+individuals a year, or (c) makes half its revenue via selling personal data.

GDPR

Protects consumers in the E.U., and applies to any company selling products/services to customers inside the E.U. Regardless of size or the company's data activities (i.e., whether or not they sell customer data), anyone processing/controlling data collection from/in the E.U. is under the jurisdiction of GDPR.

www.xtivia.com
888-685-3101 ext. 2

Data Information / Focus

CCPA

Concerns any information that could be reasonably linked (directly or indirectly) to a C.A. consumer.

GDPR

Primary focus is "**personal data**," which is defined as "any information relating to an identified or identifiable natural person ('data subject')."

Right to Be Forgotten (Data Erasure / Deletion)

CCPA

Applies solely to information collected directly from the consumer (consumer data collected via a third-party does not apply), and can be deleted so long as it isn't necessary for the following:

- Completing a transaction
- Security assessments (protecting against fraud and other illegal activity)
- Identifying and repairing errors in service functionality
- Exercising free speech or other U.S. citizen rights
- Complying with legal obligations
- Using the consumer's data as it complies with the company's terms of use

GDPR

Applies to any information concerning the "**data subject**." Personal data must be erased upon request when data retention is longer necessary (regarding the initial purpose of collection), processing was consensual, and no further processing is required, or data has been unlawfully processed or collected.

Data controllers aren't required to delete data if it's necessary for the following:

- Exercising their right to free speech/ freedom of expression
- Complying with an E.U. law or other legal obligation
- Reasons connected to medicine/public health
- Archiving scientific, historical, or statistical purposes (i.e., consensual surveys or polls)

Data Protection Impact Assessment (DPIA)

CCPA

Currently, CCPA has no DPIA required by any collector/processor of personal data. However, it does maintain that companies implement security procedures and best practices regarding information collection.

GDPR

Any company that is processing E.U. data subject information that could risk the subject's rights requires DPIAs.

Data Access and Disclosure

CCPA

At or before collection, businesses are required to inform consumers what categories of data they collect, why, and how that data will be used. If a consumer requests to see all that information, businesses have 45 days to respond to their request (covering data collected 12 months prior to request) with full disclosure (with one 45-day extension per request).

GDPR

When data is collected, businesses must inform the data subject of their privacy rights, and the subject can request access to said data at any time. If data is public, there are other stipulations. When a request is made, businesses have one month to respond and have a two-month extension if they inform the subject.

Data Portability

CCPA

The CCPA does not explicitly promote the right to data portability; however, consumers can request for the information to be sent electronically or through the mail. If the request is returned electronically, it must be portable.

GDPR

In the event of a subject requesting their data, the data processor/controller must return the information in a portable, easily readable form. In other circumstances, there are further extensions of this law.

Opting Out Requirement

CCPA

C.A. consumers can opt-out of the sale of their data, but they cannot opt-out of the collection of their data. Any organization conducting business in C.A. must inform site visitors of this in some form or another.

GDPR

Any data processing can be restricted upon request if the data subject disputes the accuracy of the data collected, data is processed unlawfully, or the processing is completed, and there is no more use for retention.

ABOUT XTIVIA

Since 1992 XTIVIA has established a proven reputation as a company that delivers leading-edge IT solutions and technology support for our clients' specific requirements, regardless of chosen technology or project complexity. Our service areas include Mobile AppDev, BI/DW, CRM, Database Support, EIM, ERP, Cloud, and Digital Experience Solutions. If you can imagine the business outcome, XTIVIA can create it with technology. We have offices in CO, NY, NJ, TX, VA, MO, and India. https://www.xtivia.com