GDPR and CCPA: How and where do they differ?

Privacy has become an increasingly important aspect of online life. In a recent survey, almost three-quarters of US consumers believe privacy laws are not good enough.

As greater amounts of personal data are generated, regulations evolve to protect the privacy rights of the individual. Two of the most well-known data privacy laws are the EU's GDPR (General Data Protection Regulation) and the Californian CCPA (California Consumer Privacy Act). These two regulations have stringent requirements on how personal data is used, shared, consumed, analyzed, and stored.

Both regulations are now several years old. Here we explore where these laws converge and where they diverge and some of the latest developments in the world of data privacy as seen through the lenses of the GDPR and CCPA.

Are the GDPR and CCPA the same?

In answer to the question in the title, are the GDPR and CCPA the same, the simple answer is in some ways, yes. The CCPA is sometimes described as GDPR2 but differs in the details and the scope of the law. The CCPA has also been criticized for being less stringent than GDPR; however, the CCPA is being updated to address some of the criticisms (this will be discussed later). To understand where the two regulations converge and diverge, the devil in the detail needs to be explored.

Where the GDPR and CCPA converge and diverge

The data (types of data covered)

CCPA: Personal information that can be used to track, link, and identify an individual consumer or a household. The CCPA covers data entered in online forms or collected by tracking cookies or similar. The act lists the data covered and includes name, social security number, address, etc.

GDPR: personal data that identifies, describes, or is associated with a data subject (individual). Includes categories for personal and sensitive data: personal data includes name, address, date of birth, etc., sensitive data includes health data, biometrics, religious beliefs, etc.

Converge/diverge: Very similar. The CCPA does not specify different requirements for sensitive data. However, there are requirements that preclude the use of data to discriminate. The CCPA defines data linked at the household or device level.

Data rights

CCPA: The right to:

- opt out
- notice (right to be informed)
- disclosure
- deletion
- equal services and prices

GDPR: The right to:

- be informed

- access
- rectification
- erasure
- restrict processing
- data portability
- object

Converge/diverge: similar but GDPR goes further in the right to object to data processing, especially for automated profiling purposes. The CCPA has consumer rights at its heart so has a right to equal services and prices.

The geography (the countries/areas covered)

CCPA: California residents but global as any business that carries out a data transaction involving a California citizen is affected

GDPR: EU residents but global as any business that carries out a data transaction involving an EU citizen is affected

Converge/diverge: both have global implications even though they are designed for specific geographies.

The organizations (business vs. data controllers)

CCPA: applies to "for-profit" organizations that do business in California. Also has provision for service providers (organizations that process personal information on behalf of a business.). For CCPA to apply a company should:

- Have gross revenues over $25 million
- Buy or sell the personal data of 50,000+ California consumers, households, or devices, per year, OR
- Receive more than 50% of annual revenue from selling California consumers' personal data

GDPR: defines data controllers **(**organizations that process personal data) and processors (organizations that process personal data on behalf of controllers.) There are some derogations for companies with less than 250 employees, mainly around reduced documentation, and reporting requirements – further details can be found in Article 30 of the GDPR.

Converge/diverge: GDPR has a wider scope and includes all organizations but with some derogations for size.

The people (consumers vs. data subjects)

CCPA: applies to California residents (even if they are transacting outside of the state). The CCPA refers to people as 'consumers' and uses the term 'household'.

GDPR: applies to EU residents. The GDPR refers to people as 'data subjects.

Converge/diverge: both cover children, but the GDPR has a wider scope for parental consent applying to all data processing consent requests.

The technology (pseudonymization, anonymization, encryption)

CCPA: deidentified or aggregated data is the baseline technological measure under CCPA. However, there are stringent definitions on how this is achieved.

GDPR: only anonymous data is exempt.

Converge/diverge: both require technical controls such as encryption and robust authentication

Opt-in or out?

CCPA: requires businesses to show privacy notices with an explicit opt-out option

GDPR: default and explicit opt-out by data controllers when collecting personal data

Converge/diverge: both are similar but the CCPA notice requirements only cover 12-months after the request

Breach notification

CCPA: breaches must be reported to the California Attorney General within 72 hours of noticing the breach.

GDPR: a data controller must report a personal data breach to its local supervisory authority within 72 hours of becoming aware of the breach (if it is likely to result in a risk to the rights and freedoms of individuals.)

Converge/diverge: both are similar

Fines

CCPA: The maximum charge per violation is $7,500 for intentional violations, or $2,500 if non-intentional.

GDPR: Up to €20 million (euros) or up to 4% of a company's global annual turnover., depending on the violation type. Recently, Amazon was fined $887 million for the use of data for targeted marketing.

Converge/diverge: CCPA fines are lower than GDPR, however, the latest update to the CCPA (see later) may change this.

What's new in the world of GDPR and CCPA?

Privacy laws reflect the status of technology and consumer expectations. As such, these laws tend to change over time. Some updates to the CCPA and GDR are:

CCPA

The latest update to the CCPA, the California Privacy Rights Act (CPRA), sometimes called the CCPA 2.0, brings new requirements into play. This update will come into force on January 1, 2023. Changes

include a threshold increase in the number of consumers whose data is processed from 50,000 to 100,000. The update also includes more stringent consumer rights that are more in line with the GDPR.

GDPR

Enforcement of GDPR is increasing in pace and moving from breach notification fines to fines for non-compliance with data rights and the legal basis for processing. New legislation is also entering the landscape, e.g., NIS2 ((Network and Information Security (NIS) Directive), DGA (Data Governance Act), and the ePR (ePrivacy Regulation): these regulations bolster and augment GDPR requirements.

Data transfers between the EU and the US

Cross-border transfers of data are a complex area, even if both sides have equivalent privacy laws. Data transfer is increasingly a global issue and can cause business bottlenecks. To alleviate this, jurisdictions create legal frameworks to help data movement flow.

Data transfers between the EU and the USA are covered by EU standard contractual clauses (SCCs), which came into force in 2021. These contracts are used to cover the complicated legalities of the transfer of personal data from the European Union to third countries. Existing EU SCCs are valid until 27 December 2022, after which they need to be replaced.

Why privacy matters, globally

Privacy regulations the world over reflect the massive amounts of personal data collected, shared, transferred, analyzed, and stored by businesses. These regulations are legal requirements, and if a business comes under the umbrella of privacy law, it must comply or face large fines. Even seemingly local laws such as CCPA can have global repercussions because businesses often act globally. But privacy is not just about avoiding fines. Our customers want the respect for their privacy. As a McKinsey insight "The consumer-data opportunity and the privacy imperative" found out:

"*Consumers trust companies that limit the use of personal data and respond quickly to hack and breaches*".

The march of privacy continues: new state laws are expected to come into force in the USA in the coming 18-months, including in Virginia, Colorado, and various others

The new tech era of the Metaverse and Web 3.0 will ensure that privacy laws like GDPR and CCPA will continue to change to reflect these paradigms. Keeping pace is now an integral part of doing business the world over.