CCPA vs GDPR: similarities and differences

As companies face potentially new, strict data privacy laws implemented by the European Union and the State of California, let's take a moment to understand the similarities and differences between the CCPA and GDPR.

The European Union's General Data Protection Regulation (GDPR) went into effect on 25 May 2018, and the California Consumer Privacy Act (CCPA) went into effect on 1 January 2020. While substantial similarities exist between the two—after all, the drafters of the CCPA looked to the GDPR while creating the CCPA—there are also substantial differences. We will explore both below.

Covered Businesses

The GDPR and the CCPA both regulate companies operating outside of their borders. However, the legal basis used to determine coverage of each law is substantially different.

Data controllers and data processors established in the EU that process personal data in the context of their activities in their EU establishments are subject to the GDPR regardless of whether they process the data inside an EU Member State or abroad. Being established in the EU is a low threshold—entities with European branches, subsidiaries, employees, or agents in the EU qualify as being "established" there based on pre-GDPR case law.

For companies that are not established in an EU Member State, GDPR compliance is still required if they process the personal information of EU data subjects in connection with offering goods or services in the EU or monitoring the behaviors of data subjects in the EU.

The GDPR does not make exceptions for small or non-profit organizations. The CCPA attempts to be more business- and charity-friendly by restricting its coverage to for-profit businesses* that handle the personal information of California residents and also do at least one of the following:

1. Make over $25 million in revenue (not profit) per year

2. Handle the personal information of 50,000 or more people, devices, or households from California per year

3. Make at least half of their revenue from selling Californians' personal information

Any organization that meets the threshold is considered a 'covered' entity, but it need only offer CCPA protections to Californians data subjects.

Who do the laws protect?

Both the GDPR and CCPA are designed to protect individuals in their territorial jurisdiction, but the nature of their relationship with the jurisdiction can be quite different.

CCPA and California Residents

The CCPA only protects Californians because the law only protects 'consumers,' which it specifically defines as 'California residents.' Therefore, a resident of an EU Member State visiting California would not receive CCPA protections, even if he interacted with a CCPA-covered entity.

On the other hand, a Californian visiting an EU Member State would have the right to CCPA protections from any CCPA-covered entity, whether she interacted with the entity while in California or while in Europe temporarily. If she relocated to Europe and became a European resident, she would lose the right to CCPA protections.

Data Processing and the GDPR

The GDPR refers to the individuals it protects as "data subjects." EU Citizens and residents are the intended beneficiaries of the GDPR. The GDPR, however, can apply much more broadly because it focuses on whether the data processor or controller was covered, not on where the data subjects reside.

This means the GDPR can technically apply to *anyone*, even visitors, in Europe.

To take it a step further, the GDPR can also apply to non-European data subjects who never step foot in Europe if a non-European data controller off-shores its data to a European data processor. For example, imagine a US company collects personal information in the US from US data subjects and then sends the information to a European data processor. That data is now subject to GDPR protections, even if the data subjects themselves were in the US when their data was collected.

Consider this example:

- A California resident visiting France who used a social media app while there and received geo-locational targeted ads would be able to claim GDPR rights as regarding the data the app collected while she was in France.
- A resident of France visiting California using the same app and receiving geolocation-targeted ads would not be able to claim CCPA rights.

So, while both the CCPA and the GDPR look to location, the CCPA looks to the *location of a person's residence* while the GDPR looks to the *location and activities of the data processors and controllers*.

What rights do protected individuals have?

Under the CCPA, California residents have the right to:

1. be given notice at or before the point of collection of their personal information;

2. know what information an entity has collected about them (commonly referred to as a Right to Know);

3. request deletion of their personal information; and

4. opt out of the sale of their personal information (opt in to sale rules may apply to minors or their guardians).

The GDPR gives similar but more expansive rights to the consumers (referred to as 'data subjects') it protects. People protected by the GDPR, like California residents, have the right to:

1. notice regarding the collection and processing of their data and their related rights;

2. know what information an entity has collected about them (commonly referred to as a Right to Know); and

3. the erasure of the personal information a company has collected about them.

The GDPR also grants individuals additional rights. While the GDPR does not offer an explicit opt-out of sale right the way the CCPA requires, the GDPR does gives protected individuals the right to restrict how their personal information is used. That right allows them to essentially opt out of sale via processing restrictions. They can opt out of the processing of their data for marketing purposes or opt out of processing activities altogether.

The GDPR also restricts the ability of controllers and processors to engage in solely automated processing if the processing produces legal effects or significantly impacts individuals. For example, if an individual applies for a loan online and an algorithm decides whether the loan will be made, that is solely automated processing. If a human decides whether to issue a loan based on, among other things, a profile created by the purely automated algorithm, the process was not solely automated.

Additionally, the GDPR gives protected individuals the right to the correction of inaccurate data and the completion of incomplete data that a covered entity has collected about them.

The GDPR also grants the right of data portability, which allows individuals to have their data transferred from one electronic processing system into another.

The Takeaway

Both the CCPA and GDPR require businesses to undergo changes to become compliant. They include (but are not limited to) all sorts of new needs that range from creating and following cookie policies, appointing Data Protection Officers (DPOs), and conducting Data Privacy Impact Assessments (DPIAs) under the GDPR to registering as a data broker (even if you don't think you are one), creating new privacy policies, and creating a data map to track your organization's data under the CCPA.

The rights offered to protected individuals under the CCPA and the GDPR are expansive, and they require a significant lift for companies trying to comply with one or both laws. The actions you take to fulfill one law will not bring you into full compliance with the other, but the lessons learned as you comply with one will definitely help you comply with the other. As your organization works toward CCPA and/or GDPR compliance you will become more:

1. savvy regarding privacy protections across complicated legal regimes;

2. transparent in your treatment of consumer data; and

3. efficient in the process of tracking and responding to consumer data requests based on their expanded privacy rights under the CCPA and the GDPR.