COMPARISON

Comparison of the European GDPR and the Californian CCPA

Why

Both regulations are in place to guard private citizens' data privacy and protect data security. The EU's General Data Protection Regulation (GDPR) is a binding regulation for all member states that has become a standard and must be adhered to by all firms. Here, we examine the differences and similarities between it and the US state of California's new California Consumer Privacy Act (CCPA).

Contact us:

info@drkpi.com
+41 44 2721876

CyTRAP Labs GmbH
Röntgenstrasse 49
CH-8005 Zürich

When comparing the European Union's General Data Protection Regulation (GDPR) with the California Consumer Privacy Act (CCPA), we need to keep in mind:

- **GDPR** is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU). On 1 January 2019, the population of the EU was estimated at 513.5 million inhabitants.

  The GDPR is all about protecting the private data and personal information (PI) of "natural persons" (individuals) who reside in the European Union. Those collecting data may be businesses, public bodies and institutions that are established inside and / or outside of the union.

- **CCPA** is a law designed to protect the data privacy rights of citizens living in California. On 1 January 2019, the population of California was estimated at 39.9 million inhabitants. In short, the CCPA forces companies to provide more information to consumers about what's being done with their data and gives them more control over the sharing of their data.

  The real issue that the law addresses is that most consumers don't realise that their personal information is being shared or sold to others. In turn, consumers have the right to know which information is being sold and to whom, and that they can opt out of allowing that information to be sold. Finally, they have the right to receive equal service and price regardless of whether they exert the rights under CCPA or not.

Contact us: info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Both laws

1. Give individuals the right to view and access the data companies collect on them.
2. Ensure that individuals are given the chance to opt out of having their information used in a way that they disapprove of.
3. Require businesses to delete personal data upon request (with some exceptions).
4. Force businesses to disclose specific details on how they handle personal data.
5. Permit businesses to ignore both laws but only for specific defined reasons (e.g., law enforcement).
6. Make certain that businesses who do not comply will be fined. GDPR fines are higher than those levied under the CCPA. Consumers can also seek much higher compensation for violations under the GDPR. Under the CCPA, typical fines range from $100 - $750 per consumer, per incident or actual damages, whichever is greater.
7. Require businesses to implement some (not specified) cyber security measures.

Additional points that matter

1. Regardless of where your company is located, the CCPA protects Californians' data while the GDPR protects the personal data of any individual residing in the EU.
2. The CCPA only applies to for-profit business and small businesses may be exempt, while the GDPR applies to any virtual business, organisation, or institution that collects, processes, or operates with the data of people located in the European Union.
3. The GDPR requires data protection officers and additional processes and paperwork, such as maintaining a record of an audit or audit certification. Audit documentation can be a collection of processed activities conducted for the execution of data protection, an impact or risk assessment, or similar. The CCPA doesn't require any such appointments or processes.

Contact us: info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

A Few Final Takeaways from Our Look at the CCPA vs GDPR

Although the CCPA awards greater rights to a smaller group of individuals and affects fewer businesses than the GDPR, it is still a powerful piece of legislation that is expected to have a major impact on businesses worldwide. And while the regulations your business may have implemented to comply with GDPR from May 2018 are helpful, they will not encompass all necessary updates or changes you should have taken care of for the CCPA before January 1, 2020. The law allows Californians, known for being litigious, to sue businesses if their personal information is compromised in a data breach.

As well, aside from requiring organisations to conduct risk assessments and adopt necessary security measures, neither the CCPA nor the GDPR provide much in terms of how to approach risk mitigation in data processing. Here we provide you with a short list of our own recommendations (more upon request):

- Keep all private and personal information encrypted; be secretive about passwords.
- Implement strong access control mechanisms, policies, and procedures.
- Teach employees cyber security best practices and provide cyber awareness training.

---

[1] In order to be considered a covered business, the organisation needs to have annual gross revenues in excess of $25 million, possess the personal information of 50,000 consumers, or derive 50 percent or more of its annual revenue from selling consumers' personal information. It is the data collection threshold of 50,000 people that is expected to catch many small businesses that do not have $25 million in revenue. If you are collecting IP addresses on 137 visitors to your website a day, then you would have the requisite amount of data collection over the course of a year to be considered a business under the CCPA.

For more questions and a suggestion on how to conduct a data protection audit, you can consult our webpage or contact us directly from there: https://drkpi.com/
You can also send us an e-mail or call us (see footer below).

Contact us: info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich