Comparison of GDPR and CCPA

Four Quick Thoughts and Takeaways

Since the European Union's General Data Protection Regulation (GDPR) went into effect in May 2018, more and more governing bodies are looking at ways to provide individuals protection through data privacy laws.

The California Consumer Privacy Act (CCPA) is a prime example and will go into effect in January, 2020. These two regulations are poised to greatly influence privacy protection practices around the world and are generating great interest from businesses and the public.

While there are certain to be changes and finer interpretations as the laws are enforced and challenged, we created this quick overview of four areas where GDPR and CCPA cover similar topics, though perhaps in slightly different ways.

Scope

What Entities are Covered?

GDPR is has a broader scope of covered entities, including not just businesses, but also public entities and non-profits, who offer goods and services within the EU. CCPA covers businesses that collect data of California consumers.

Who is Covered?

CCPA covers "consumers" who are natural persons and residents of California. GDPR covers "data subjects," but is far less restrictive in terms of residency requirements.

What Data is Covered?

GDPR is very broad in the data covered, while CCPA excludes data covered by U.S. federal law from its scope, such as HIPAA.

Personal Data

While both GDPR and CCPA have very broad definitions of personal data, CCPA reflects the concerns of selling data and has specific requirements related to data selling and transfer due to mergers and acquisitions activity. For example, CCPA requires a "Do Not Sell My Personal Information" link to be included on the homepage. Pseudonymisation, though too complicated to address in detail here, is treated similarly in both GDPR and CCPA.

Consumer Rights

The rights of consumers are similar in GDPR and CCPA and include the right to have data deleted, right to be informed of the data and its uses, the right to opt out, a right of access and the right to port data. CCPA also includes a right to ensure consumers are not discriminated against for the exercise of rights under the law.

Interestingly, GDPR requires that companies have some "legal basis" for any processing of personal data, but that is not the case in the CCPA.

Remedies and Penalties

Perhaps the most eye-catching provision in GDPR is the monetary penalty of up to 4% of annual global sales or €20 million, whichever is higher. GDPR imposes this as an administrative fine. CCPA allows for an expanded private right-of-action and civil penalties up to $2,500 for each violation or $7,500 if the violation is "intentional." Though the amounts seem small when considered as a singular amount, CCPA does not have a cap to the penalties, which are calculated on a per-violation basis, so class action suits involving many violations can certainly add up.

From a governance perspective, GDPR requires the appointment of Data Protection Officers as well as maintaining defined reports. CCPA is not specific on roles or reports, but requires other steps to ensure compliance such as training of staff.

Data Privacy

Our solution

While many organizations have taken on privacy impact assessments, we are operationalizing data privacy compliance with Conduent technology and workforce. Savvy organizations recognize that they will see a significant uptick in consumer and employee requests to exercise rights over their personal data. The recent Facebook data breach impacted more than 87 million users, and more California residents than any other. In a recent survey of EU citizens, more than 50% of respondents stated that they intended to exercise their GDPR rights through subject-access request.

While data mapping and scanning software exists, its one-size-fits-all approach is prone to error, can miss critical elements, and standing alone cannot do more than provide users with a status report.

We partner with our clients to ensure we have all the proper classification models and search terms required to identify and capture all relevant personal data. We do this by mapping entire corporate data stores where exposure is likely to occur and applying analytics schemas for personal data identification. We also review and prioritize data sources based on probability of personal data and determine the accessibility of the source.

We partner with our clients to ensure all proper taxonomy and classification models are applied, as well as search and retrieval algorithms to identify and capture all relevant personal data.

With our data privacy solution, companies can:

- Identify risky practices in their organization that affect employee or consumer privacy rights
- Respond to consumer requests for their personal data
- Protect against risk of shadow data stores containing protected personal information
- Leverage advanced data science-based approaches to managing employee and consumer personal information
- Provide additional support for certification of compliance with subject-access requests
- Deploy repeated and ongoing audit and governance of corporate compliance with organizational policies
- Better manage and meet the operational burden of increased subject-access requests • Optimize future data storage
- Proactively identify and remediate areas of risk

Conduent provides a single, searchable database of personal information and associated data subjects found across your enterprise to help operationalize your data privacy compliance obligations, such as subject-access requests. Our solution can capture and document key information such as the personal data type, data source and processing use. For the most nuanced and specific questions and needs, our dedicated team of experts can design complex analytics against virtually unlimited fields of data to quickly and accurately comply with any demand.

A hybrid approach

Partnering with our clients to design solutions that combine analytics with IT and compliance talent, Conduent applies intelligent advanced analytics and subject matter expertise to mitigate risk, optimize performance, enhance accuracy and provide defensibility. Our big data analytics platform aggregates metadata from many sources and stores it in a single, secure repository — located in a deployed appliance in a regional certified cloud or in one of our global ISO 27001 data centers.

Conduent's approach includes:

- Simple and complex analytical search capabilities across all company data sources
- Rapid identification of risk factors
- Insights and summaries of personal data patterns
- Visualizations to quickly view important flags for action such as heat maps, concept clouds, time series analysis and more
- Clear identification and reporting of documents flagged for specific needs

Learn more

For more information on Conduent Legal and Compliance Solutions, visit us at: www.conduent.com/solution/legal-business-solutions or call **1-844-ONE-CNDT**

CONDUENT