California Consumer Privacy Act (CCPA)

The continued convergence of the regulatory landscape and personal data.

The General Data Protection Regulation (GDPR) caused a seismic shift in the regulatory landscape across Europe. It grabbed headlines — and the attention of boards everywhere. However, it’s now the California Consumer Privacy Act (CCPA) 2018 that’s moved into the spotlight. CCPA is just the latest example of a global trend toward formally recognizing and codifying individual rights to privacy that were spearheaded in the GDPR. Organizations globally are starting to face the reality that, in the wake of recent data breaches and the negative public reaction, regulatory requirements are becoming more prescriptive and consumer tolerance for poor data handling practices is lower than ever. Adapting to this change is not an option — it is critical to survival.

Despite these seismic shifts in the regulatory landscape and the mounting sentiment that consumers don’t trust companies with their personal information, organizations are continuing to demand that consumers share more and more personal information. Yet, 77 percent of people surveyed in European Commission Eurobarometer say that the disclosure of information is a big issue for them and they are concerned about not having full control over the information they provide online. As companies move toward a more digitally enabled landscape, the processing of this personal information is becoming a fundamental part of how organizations deliver their core services to consumers. While many organizations are working towards, or have achieved, a defensible compliance position, the most successful organizations will be those that transform the way they manage and use data to maximize its value while building and maintaining consumer trust and loyalty. In order to take advantage of such rules, the time to start thinking about privacy is now.

The passing of the CCPA is a landmark moment for US privacy law

For many US companies, the regulatory upheaval caused by the GDPR was barely felt — a distant rumble of thunder that could be ignored or easily avoided. The requirements perhaps didn’t apply at all, or elements of the business could be ring-fenced to limit the impact.

The CCPA will change this. It is a comprehensive specific law that spans all industry segments with similar requirements to the GDPR and impacts all organizations.
that process personal information of residents of California. The CCPA is the first law of its type in the US and will give some US citizens similar rights to their counterparts in Europe.

Key obligations under the CCPA include:

- notification to the regulator of breaches of personal information it may have had. It is important to note this is a not a new requirement in California as notification was required under the California Data Breach Notification Law

- providing certain rights to consumers over their personal information such as:
  - knowing what personal information is being collected
  - knowing to whom their information is being disclosed
  - opting-out of the sale of their personal information
  - accessing their personal information.

Importantly consumers under the law are afforded Equal service regardless of whether these rights have been exercised.

The CCPA is representative of a wider sea change. California is one of the largest economies in the world, but all companies will have to better understand their data practices and the impact of such regulations on their business strategy. Waiting to the last minute is not a viable option.

Doron Rotman
America Privacy Advisory Co-Lead

How does this affect my organization?

The impact of this law will depend on the specific circumstances of your organization. There are three likely scenarios:

Scenario 1 — CCPA is applicable, but GDPR isn’t. In this scenario, the passing of the CCPA is likely to have a significant impact. Having not been impacted by similarly comprehensive privacy laws previously, putting your organization in a position to meet the requirements of CCPA is likely to require significant investment. Decisions will need to be made around whether you seek to ring-fence elements of your business to minimize the impact of CCPA, or adopt more robust privacy practices across your entire organization.

California is at the center of the person information universe with billions of individuals personal information records flowing through California based organizations products and services on a daily basis. The CCPA’s alignment with the GDPR demonstrates the convergence that is occurring across the world in respect of the regulatory landscape and in the expectations of individuals when their personal information is processed.

Mark Thompson
Global Privacy Advisory Lead

— notification to the regulator of breaches of personal information it may have had. It is important to note this is a not a new requirement in California as notification was required under the California Data Breach Notification Law

— providing certain rights to consumers over their personal information such as:
  - knowing what personal information is being collected
  - knowing to whom their information is being disclosed
  - opting-out of the sale of their personal information
  - accessing their personal information.

Mark Thompson
Global Privacy Advisory Lead

How does this affect my organization?

The impact of this law will depend on the specific circumstances of your organization. There are three likely scenarios:

Scenario 1 — CCPA is applicable, but GDPR isn’t. In this scenario, the passing of the CCPA is likely to have a significant impact. Having not been impacted by similarly comprehensive privacy laws previously, putting your organization in a position to meet the requirements of CCPA is likely to require significant investment. Decisions will need to be made around whether you seek to ring-fence elements of your business to minimize the impact of CCPA, or adopt more robust privacy practices across your entire organization.

California is at the center of the person information universe with billions of individuals personal information records flowing through California based organizations products and services on a daily basis. The CCPA’s alignment with the GDPR demonstrates the convergence that is occurring across the world in respect of the regulatory landscape and in the expectations of individuals when their personal information is processed.

Mark Thompson
Global Privacy Advisory Lead

— notification to the regulator of breaches of personal information it may have had. It is important to note this is a not a new requirement in California as notification was required under the California Data Breach Notification Law

— providing certain rights to consumers over their personal information such as:
  - knowing what personal information is being collected
  - knowing to whom their information is being disclosed
  - opting-out of the sale of their personal information
  - accessing their personal information.

Importantly consumers under the law are afforded Equal service regardless of whether these rights have been exercised.

Doron Rotman
America Privacy Advisory Co-Lead

The CCPA is representative of a wider sea change. California is one of the largest economies in the world, but all companies will have to better understand their data practices and the impact of such regulations on their business strategy. Waiting to the last minute is not a viable option.
It is important to recognize that getting privacy right isn’t just about getting your own house in order. Organizations are reliant on an increasingly complex supply chain that needs to be just as robustly secured. We’ve seen countless incidents where weaknesses in the supply chain have been exploited with devastating consequences.

**Trust isn’t established with a paper shield**

Too often, organizations approach privacy as an exercise in establishing a defensible position — little better than box ticking. In today’s information sharing and information-dependent economy, data is the new currency. Organizations that proactively manage and protect personal information the way consumers expect will come out ahead of their competition.

Trust is critical and it isn’t built on a paper shield. Organizations need to transform how they manage privacy to enable value creation from data in a way that enhances consumer trust.

---


---

**Scenario 2 — CCPA is applicable, as is GDPR.** If you have already prepared your organization to meet the requirements of the GDPR and applied the same standard across your entire organization, the CCPA may have less of an impact. Some changes may be needed to cover the nuances of CCPA, however the alignment between the two regulations means this should be a matter of enhancements rather than wholesale change. However if your GDPR program has not covered your California operations in a meaningful way you are likely to have a significant impact.

**Scenario 3 — CCPA does not apply.** Your organization doesn’t process personal information of Californian residents and therefore may not need to make immediate changes. However, given the trend in privacy law globally, taking proactive steps now to align to the core principles would be prudent.

---

**What should I do?**

Impacted organizations will need to invest time and resources to get their personal information handling processes and controls in line with the applicable requirements. We recommend following the five step approach below.

---

**Step 1: Strategize**
- Understand your legal requirements
- Get senior level buy-in and appoint sponsor
- Set risk appetite and target state

**Step 2: Reflect**
- Assess your current state
- Map out what personal information you have and how you handle it now

**Step 3: Plan**
- Make an action plan to address the gap between current and target state
- Work out the resources you need to close the defined gap and achieve your target state

**Step 4: Deliver**
- Deliver the activities defined in your plan (e.g., updating internal policies, procedures and processes)
- Train and upskill staff to raise awareness of GDPR and new processes

**Step 5: Embed**
- Monitor controls implemented and continuously improve
- Mature effectiveness of controls through use of technology
- Undertake a program of cultural transformation to make privacy a way of life

---

Privacy done right — putting the customer at the core of your privacy strategy — is a game changer. Regulations like the CCPA, GDPR, and other similar global regulations provide incentive, but compliance should be a bi-product, not the end goal, of a well-designed privacy program.

*Orson Lucas*
America Privacy Advisory Co-Lead