Davis Brown Employment and Labor Law Blog

The Decade of Data Privacy: What the CCPA and GDPR Mean for Your Business – January 10, 2020

Shannon M Holmberg

As you fired-up your computer after last week's New Year holiday, your inbox was likely filled with emails about updated privacy policies. You may remember receiving a similar wave of emails in May 2018.

While it might seem that companies made a collective New Year's resolution to update their policies, both the 2018 and 2020 emails can be connected to two important data privacy regulations that will shape the global economy over the next decade.

In 2018, the culprit behind the wave of updated privacy policy emails was the EU General Data Protection Regulation (GDPR). This time? The California Consumer Privacy Act (CCPA).

Despite the appearance of limited geographic scopes of the EU GDPR and CCPA, both regulations have far-reaching influence that may bring your business within their grasp. As we embark on this new decade, be sure to make data privacy compliance a top priority for your business.

GDPR: The Precursor to the CCPA

The EU GDPR took effect in May 2018, prompting many businesses to update their privacy policies, resulting in a wave of emails notifying customers of changes and asking customers to consent to continued marketing communications.

The GDPR regulates the processing of data for all EU residents by creating new data privacy rights and a severe penalty framework for violations. Under the GDPR, any organization that collects and/or processes personal data (e.g. name, email address, physical address, phone number, etc.) from EU residents must comply.

Under the GDPR, organizations must have a lawful basis for processing this information, such as consent, contractual or legal obligation, vital interest, public task, or legitimate interest. Although the GDPR is an EU regulation, organizations worldwide are subject to the requirements based upon the broad geographic scope.

Shortly after the GDPR took effect, the state of California passed regulation of its own, the California Consumer Privacy Act (CCPA).

The California Consumer Privacy Act

The CCPA became effective on January 1, 2020. Like the GDPR, the CCPA created both new rights for consumers and new penalties for businesses that fail to comply. While the CCPA is a California regulation, it reaches well beyond California's borders and could affect your business.

Is your business subject to the CCPA?

The CCPA applies to any for-profit entity (or any entity it controls or is controlled by) that:

- Does business in California; **and**
- Satisfies one or more of the following criteria:

    1. Has annual **gross revenues greater than $25 million**; or
    2. Annually buys, receives for the business's commercial purpose, sells, or shares the personal information of **50,000 or more consumers, households or devices**; or
    3. Earns **50% or more of its annual revenues** from selling consumers' personal information.

A number of Iowa businesses will be impacted by the regulation, including Iowa-based retailers or service providers who market and sell to consumers in California.

What is considered Personal Information under the CCPA?

"Personal Information" means any information identifying, relating to, describing, or capable of being associated with or reasonably linked with a particular consumer or household.

This includes identifying information such as:

- Name
- Mailing address
- Email address
- Social Security number
- IP address
- Biometric information
- Internet activity
- Geolocation data
- Professional or employment information

There are very limited exceptions when it comes to what data qualifies as personal information.

What should your business do to comply with the CCPA?

Like the GDPR, the CCPA imposes significant compliance obligations upon businesses within its scope. These obligations include providing specific privacy policy disclosures, allowing consumers to access and request deletion of their personal information, providing a mechanism for consumers to opt-out of the sale of their information, and providing consumers with the right to equal service and prices--even if they opt-out of the sale of their information.

Complying with these obligations will require businesses to review their existing data privacy practices and potentially implement new ones.

As we enter the decade of data privacy, be sure to evaluate your business's compliance with these new data privacy regulations. Here are a few resolutions to help you get started:

1. Establish a data privacy and security team
2. Review and update your data collection and sharing practices
3. Update your privacy notice/policy and website functionality
4. Update your internal operating procedures and train employees in handling consumer data and requests
5. Review and update your agreements with third parties with respect to data processing

The Big Picture: Consumer data privacy rights will continue to increase

With the implementation of the GDPR and CCPA, the scale has tipped in favor of consumer data privacy rights and increased enforcement of violations, and more states are sure to follow suit with regulations of their own. If you haven't given much thought to your business's data privacy practices, now is the time to do so.

Check back with Davis Brown for additional content and analysis regarding other developments in data privacy law. You should contact your attorney to determine whether your business needs to comply with these data privacy regulations, and what actions are needed in order to do so.
