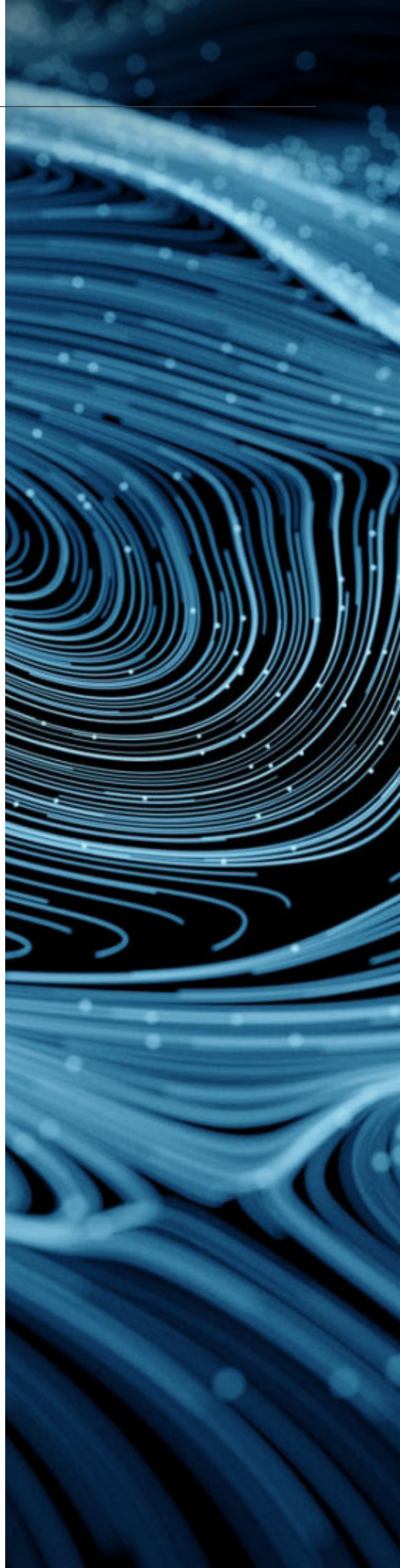
CCPA IN FULL FORCE: HOW TO GET THE SUPPORT YOUR ORGANIZATION NEEDS

BDO DIGITAL



January 1, 2020, ushered in a new era for data privacy in the United States when the California Consumer Privacy Act (CCPA) took effect, with enforcement beginning on July 1, 2020. If it wasn't enough that companies continue to struggle in the wake of a global pandemic, now they must comply with a new privacy law that is certain to bring regulatory fines and potential litigation. To ensure privacy compliance and combat potential litigation if and when they experience a data breach, organizations need to understand what data they have, how it's used and stored, and where and how it's shared.

The CCPA brings the most comprehensive privacy law in the United States by creating obligations for businesses to honor the rights of consumers, including the rights to access, delete and opt out of the sale of their data. Additionally, there is an obligation for businesses that own or license personal data to disclose a breach to any affected Californian if more than 500 residents are impacted. Despite these onerous obligations, Attorney General (AG) Xavier Becerra decided not to delay enforcement of CCPA despite industry groups pushing to do so.

Final CCPA regulations are yet to come, with a third set of modifications released on October 13, 2020, and voters passed a ballot measure for the California Privacy Rights Act (CPRA) in November. CPRA will become effective on January 1, 2021, and most compliance obligations will be required by January 1, 2023. Until January 2023, businesses need to comply with CCPA. However, there is impending fear of litigation related to both CCPA and CPRA. It's important for businesses to understand the differences between the two so they know what to do to avoid compliance and litigation costs. This article outlines the differences between CCPA and CPRA and provides an overview of what companies can do to minimize their risk of litigation and reduce costs in the event they are faced with litigation.

CCPA VS. CPRA

Although there is not a large difference in the scope of CCPA compared to CPRA, there are slight differences that are critical to grasp. The respective laws apply to organizations that meet the following criteria:

CCPA	CPRA
▶ $25 million or more in annual revenue; OR ▶ 50% of annual revenue derived from selling consumer personal data; OR ▶ Earn more than half of its revenue selling consumers' personal data.	▶ $25 million or more in annual revenue; OR ▶ Buys, sells or shares the data of 100,000+ consumers or households; OR ▶ At least 50% of annual revenue is derived from selling or sharing consumers' personal data.

It is almost important to recognize that CPRA establishes a new enforcement body, the California Privacy Protection Agency, which is very similar to the Supervisory Authorities under the European Union's General Data Protection Regulation (GDPR). The agency would be charged with enforcing California's data privacy laws. The CPRA also creates a new category of data, sensitive personal information, which is similar to Article 9 of the GDPR. Sensitive personal information would include social security numbers, financial information, geolocation data, genetic data and other biometric data.

INVENTORY AND CONTROL OF DATA

In an increasingly digital economy that thrives on data, all organizations bear a degree of risk in collecting, managing and using consumer data. In order to properly control and protect data, organizations need a clear picture of precisely what data they have, where it's stored and how it's used. That's why building a data inventory is central to managing consumer data, safeguarding it from a breach and complying with privacy regulations—including the need to address consumer requests to access, delete and opt out of the sale of their data. That inventory helps identify different types of data that could be linked, directly or indirectly, with a particular consumer and could be compromised in the event of a breach.

Following best practices for data management helps with the installation of strong protocols to control consumer data throughout its lifecycle. A data inventory can also help to identify data governance gaps and vulnerabilities that could lead to non-compliance. The data inventory, and records of processing activities to which the data is subject, enable enhanced data protection practices, thereby mitigating risk and allowing swift and effective response in the event a breach does occur.

CONSUMERS' PRIVATE RIGHT OF ACTION AND THE CURE PROVISION

A pivotal aspect of CCPA is the private right of action, which allows affected consumers to file class actions seeking class-wide statutory damages. These actions have a lesser burden of proof than other types of litigation. The required fine is a maximum of $750 (and a minimum of $100) per consumer per violation, so the total fine can vary depending on the size of the class. The pool of money is also uncapped, which creates the potential for massive fines to be levied in the event of a large-scale data breach.

Even before CCPA, the costs of addressing a data breach could threaten the very existence of a business. For example, the 2018 privacy breach of debt collector American Medical Collection Agency impacted more than 20 million individuals and led to the bankruptcy of its parent company Retrieval Masters Creditors Bureau. Furthermore, CCPA is far from the only legal concern, because data breaches can violate other laws as well. It's critical to understand all legislation that could apply to compromised data, such as national security violations in the event of a breach at a government contractor. Through a reputation lens, a breach can result in monetary and business impacts, which could damage strategic business relationships, result in loss of consumer trust, reduce market share and result in reputational harm.

The CCPA does have a cure provision, which affords affected organizations a 30-day window after receiving notice to avoid statutory damages by remedying any effects of a breach. If this is accomplished, the consumer can only file suit for actual damages (the amount of money lost that can be proven to be the direct result of the data breach), but not for statutory damages. The cure provision also applies when the regulator gives notice of a violation; failure to remedy the violation within 30 days can result in a fine of up to $7,500 per record. That's why being prepared to respond quickly in the event of a data incident or breach is a crucial aspect of compliance.

CONSUMERS' PRIVATE RIGHT OF ACTION AND THE CURE PROVISION

Even before CCPA enforcement began on July 1, numerous class actions had been filed against major companies, including Amazon-owned smart device maker Ring, video communication platform Zoom, social game developer Zynga, facial recognition provider Clearview AI and online stationery company Minted. Consumers' private right of action significantly increases companies' exposure to potential litigation, so it's vital to have the preparations and support in place to deal with legal action.

- Sheth v. Ring LLC, Case No. 2:20-cv-01538
- Cullen v. Zoom Video Communications, Inc., Case No. 5:20-cv-02155
- Hurvitz v. Zoom Video Communications, Inc. et al., Case No. 2:20-cv-03400
- Nasim Chaudhri and Amy Gitre v. Zynga, Inc., Case No. 3:20-cv-01539
- Carol Johnson and Lisa Thomas v. Zynga, Inc., Case No. 3:20-cv-02024
- Burke v. Clearview AI, Inc., Case No. 3:20-cv-00370
- Atkinson v. Minted, Inc., Case No. 3:20-cv-03869

CRITICAL FACTORS IN RESPONDING TO A BREACH

If a data breach occurs, time is of the essence. The affected organization must be prepared to act quickly to communicate with internal stakeholders, restore security, assess the damage and mitigate downstream risks. Then it's necessary to notify affected parties, take steps to remedy the violation and introduce privacy and security enhancements to help avoid future breaches. It's imperative to identify necessary disclosures and act within the required notification timelines, while also identifying resources to facilitate the notification process.

Communication

Communication during a breach response is key, and there should be a comprehensive plan in place to guide and manage response activities. This includes notifying internal stakeholders, including applicable C-suite executives—especially the Data Privacy Officer and/or Chief Information Security Officer—plus general counsel and outside counsel as appropriate. Documentation is another vital aspect of the breach response. Completing an incident report can help outline the relevant details, including a description of the time and location of the event. It may also be necessary to contact law enforcement authorities, depending on the nature of the breach and the type of information that's been affected.

To communicate information externally in a clear and accurate manner, there should be an incident communication plan in place that outlines specifically how various details will be communicated. This includes responding to both consumer and regulatory inquiries. The plan should also outline how to communicate information to media sources and how inbound media requests will be handled. Failure to properly control communication can exacerbate the crisis and lead to significant reputational harm.

Incident Assessment

Assessing the damage starts with identifying the systems that have been impacted, as well as information that could have been compromised or exfiltrated from those systems. Having a data inventory prepared in advance provides key details to guide the assessment, including vendors and partners who may have access. A forensic analysis of the incident is also required to investigate the breach at a technical level. This analysis includes collecting information about the affected systems, remediating those systems and preserving other data to determine if anything has been corrupted or compromised that could have downstream impacts to other systems and data. Once the forensic analysis has been conducted, the affected systems can potentially be brought back online, if secure.

Notification

The CCPA grants consumers the right to access their personal information, regardless of whether or not a breach has occurred, so organizations need to have a corresponding process for receiving, verifying and addressing these requests from individuals. This process should be routinely tested for efficiency and effectiveness. Organizations should have a support team in place to handle and respond to these requests in a timely manner; the CCPA requires a response to all verifiable consumer requests within 45 days.

If a breach has occurred, the affected organization must enact its process for notifying victims. It should also be prepared for an increase in consumers exercising their rights and requesting information. It may be necessary to scale up the support team to respond to these increased demands. Depending on the type of information affected, it may be necessary to establish a process for monitoring the credit of affected individuals as well.

Post-Incident Assessment

Following a breach, a post-incident assessment should be conducted to identify factors that contributed to the breach and potential shortcomings in the organization's response. This assessment provides an opportunity to improve training for individual team members, increase awareness about data protection, review and upgrade policies and procedures as appropriate, and harden internal systems as needed.

SAVING COSTS WITH LITIGATION SUPPORT

In order to properly respond to a data breach quickly and comprehensively, organizations can use outside resources to assess and confirm the level of exposure. Upfront and ongoing data management practices are needed to gain visibility into the organization's exposure to potential litigation and to determine the potential scope of liability and notifications. Working with an outside service provider can also deliver integrated privacy and e-discovery capabilities to rapidly identify and understand risks and obligations as soon as possible after the incident.

The potential costs of a breach can be significant, but the costs of a slow or ineffective response can be even more substantial. According to IBM Security, the average cost of a data breach is approximately $3.9 million, and this cost can be even higher in certain industries that handle high-value consumer data, such as healthcare and financial services. Investing in a thorough and robust response plan is money well spent.

Certain tasks in a breach response can be especially costly, but there is minimal room for error; these tasks must be performed properly and thoroughly. Document review is one notable example. While the associated costs are significant, it's essential for an organization to have expert reviewers, with privacy breach response experience, to assess the extent of the breach and the organization's exposure to litigation based on the exfiltrated dataset.

Although the initial and ongoing costs of compliance are substantial, especially for larger companies, paying for expert assistance helps to avoid additional downstream risks and costs. With further guidance and recent modifications related to CCPA, compliance is an ongoing practice. Leveraging outside resources that specialize in data protection and privacy compliance helps safeguard both the organization's data and the organization itself.

BENCHMARKING DATA PRIVACY COMPLIANCE

According to BDO's 2020 Digital Transformation Survey, more than half of middle market organizations in the U.S. say they are taking steps to comply with current or forthcoming privacy regulations by providing training for employees, revising their privacy policies and processes, and updating their privacy disclosures.

Revising policies and processes for privacy—and training employees to comply with these—is a complex undertaking. As a best practice, an organization's internal privacy policy should incorporate processes to address the proportionality, adequacy, minimization, use limitation, storage limitation, accuracy, completeness, security, confidentiality, integrity and accessibility requirements for data. Using outside resources to assist with this helps expedite the process and ensure it is done correctly and comprehensively.

EVOLVING REGULATIONS FOR PROTECTING DATA IN A DATA-DRIVEN WORLD

Privacy legislation continues to be enacted, and compliance with CCPA is an important part of developing strong privacy practices and building resilience for the future. Positioning data privacy at the center of an organization's practices can be an asset for building trust with consumers and minimizing risk and exposure. It also helps prepare for future developments as consumers, lawmakers and regulators continue to scrutinize how data is collected and used.

In addition to the recent passage of CPRA, new privacy laws are being considered in other states, and some areas of data collection are getting more attention as well. One example is the proliferation of laws that regulate how entities can collect, use and share biometric data, which applies to increasingly common technologies such as fingerprint scanning, voice recognition and facial recognition. Several states have already passed biometric legislation, and others are currently considering similar measures. There is also federal privacy legislation brewing in Congress, and while this has been met with some challenges, it's an issue that has bipartisan support from lawmakers and backing from major technology companies.

All organizations should examine their data privacy practices in light of mounting regulatory scrutiny and potential litigation. Spending now on privacy compliance and preparedness helps avoid far more significant costs downstream, and it can build trust and goodwill with consumers and stakeholders as well.

Learn more about how BDO's Governance, Risk & Compliance practice can address your organization's needs related to CCPA and data protection.

CONTACTS

KAREN SCHULER
Principal, Governance, Risk & Compliance National Practice Leader
301-354-2581
kschuler@bdo.com

MARK ANTALIK
Managing Director, Governance, Risk & Compliance
617-378-3653
mantalik@bdo.com

JENNA AIRA-VENTRELLA
Managing Director, Global E-Discovery Services Leader
310-557-8256
jaira@bdo.com

BDO Digital, LLC is a Delaware limited liability company, and a wholly-owned subsidiary of BDO USA, LLP.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information on BDO Digital, LLC please visit: www.bdo.com/digital.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2020 BDO USA, LLP. All rights reserved. www.bdo.com