JANUARY 21, 2021

Legaltech news ONLINE

An ALM Publication

CCPA Vendor Management: Potential Gaps in Your Privacy Compliance Strategy

Both GDPR and CCPA make it clear that an organization is fully responsible for the vendors within their supply chains, and the onus is on those organizations to ensure compliance. Most companies don't realize the significance of this mandate and have taken little to no steps to ensure compliance.

BY RICH VESTUTO, DUFF & PHELPS AND WAYNE MATUS, SAFEGUARD PRIVACY

Many organizations have spent substantial resources to ensure internal compliance with GDPR and will spend even more to comply with the CCPA in the coming year. **According to an economic impact study** commissioned by the California Department of Finance, the initial costs to American businesses could exceed $55 billion, with some organizations spending $2 million or more to ensure their operations follow the new privacy regulations.

Many will spend quite a bit more. Organizations with over $1 billion in revenue are **estimated** to spend between $10 to $100 million to prepare for the CCPA. These estimates include a minimum of ten new fulltime hires dedicated to compliance. Much of those resources will be used for addressing customer complaints, a task to which organizations will apply people, process and technology.

But these efforts still leave a gaping hole in compliance: their vendors. Both GDPR and CCPA make it clear that an organization is fully responsible for the vendors within their supply chains, and the onus is on those organizations to ensure compliance. Most companies don't realize the significance of this mandate and have taken little to no steps to ensure compliance. This creates substantial reputational, regulatory and financial risks.

Ensuring vendor compliance is difficult in today's environment and will continue to become more complex. The privacy frameworks many organizations relied upon ceased to be useful once California and Nevada passed laws imposing defined standards to which all companies and vendors must adhere. Moreover, those frameworks are not likely to accommodate the patchwork of requirements under debate in state houses across the country.

For organizations to achieve compliance they will need to assess, in clear terms, how each

vendor adheres to specific privacy regulations.

The Onus of Vendor Management for CCPA and GDPR

Is an organization liable for the actions of its vendors under GDPR and CCPA? The answer is yes, under both laws.

GDPR Article 24

Under GDPR, the corporation is responsible for its vendors if that corporation determines the "purposes and means" of processing the consumer data. In other words, if a company opts to collect consumer data for marketing purposes they're responsible for ensuring that all vendors aiding in marketing initiatives are fully compliant with GDPR, as stated in article 24:

"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation."

Recital 74 expressly states that the "controller" is completely responsible and liable for processing done on its behalf by a third party:

"The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons."

This means if you're the entity that determines purposes and the means with which data is collected, you are responsible for ensuring all the rights described in the previous section are protected. You are also responsible for ensuring and demonstrating the vendors you rely on—data company, media agency, trading desk, benefits administrator, affinity programs, ad exchange, etc.;—process consumer data in compliance with GDPR.

CCPA and Agency Law

The CCPA analysis is a bit more complex. The CCPA defines two types of vendors: third parties and service providers. Third parties can be anyone with whom the business shares personal information: for example, an advertising network, ISP, data analytics provider, social network or data broker. Service providers are third parties that process personal data on behalf of the business, pursuant to a written contract prohibiting use of that personal data for any purpose beyond what is specified in the contract. §§1798.140 (v)(w).

Third parties and service providers are each "agents." Under agency law, a principal is responsible for the actions of their agents. The law of agency is based on the Latin maxim "Qui facit per alium, facit per se," which means "he who acts through another is deemed in law to do it himself."

California Civil Code §2338 adopts this and states: "Unless required by or under the authority of law to employ that particular agent, a principal is responsible to third persons for the negligence of his agent in the transaction of the business of the agency, including wrongful acts committed by such agent in and as a part of the transaction of such business, and for his willful omission to fulfill the obligations of the principal."

Where the entity hired is a third party, agency law applies and the business is fully responsible for negligence.

Where the entity hired is a service provider, the CCPA protects the business from liability for CCPA violations by the service provider provided that at the time of the violation, the business does not have actual knowledge or reason to believe that the service provider intended to commit the violation. §1798.145(j) states:

"A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title."

While this may seem to provide protection, it is going to be unusual for a business not to know what their vendor is doing or at least have reason to know.

Data Privacy in Vendor Contracts

To ensure vendors protect client data to the level required by both GDPR and CCPA regulations, prudent companies are **contractually obligating that protection**. Whether it is by adding new privacy clauses to new vendor contracts going forward or amending current contracts, companies are holding their vendors to the task. Oftentimes, those clauses also mandate periodic privacy compliance assessments.

Complexity of Emerging Privacy Regulations

The GDPR and CCPA are just the beginning of consumer privacy protection. Soon, organizations operating in the U.S. are likely to face a patchwork of federal and state privacy regulations. In May 2019, Nevada adopted **new privacy legislation** and included a consumer opt-out right. Additionally, legislators in 14 other states **across the country** have recently proposed their own CCPA-like privacy bills.

To say that privacy regulations are a bit of a moving target is an understatement. The Washington Privacy Act failed on two occasions to pass the legislature, but we can expect advocates to keep trying. The Texas Privacy Protection Act also failed to set specific policy to date, but it did establish a Privacy Protection Advisory Council to study data privacy laws in advance of the next legislative session. Vermont Security Breach Notice Act expands the definition of personally identifiable information to protect consumers in case of data breach.

Each act defines specific requirements, meaning businesses must adhere to the letter, and not the spirit, of each law. Failure to monitor vendors will mean the business isn't in compliance with the regulations. The frameworks once relied upon ceased to be effective once the CCPA and Nevada laws passed, imposing defined standards that the frameworks don't meet.

The Way Forward: Standardized Vendor Management

As we've seen above, businesses are liable for their third-party vendors and partners. "Reason to believe" is all too easy for a consumer to allege (for instance, a customer can claim a business "ignored my complaints"). To reduce such risks, all businesses that engage in online advertising and marketing must be able to prove they did not have a "reason to believe" a vendor violated any privacy regulations when processing data.

There's one way that companies can address that vulnerability, and that is to develop an agreed upon vendor assessment, with precise language, that discloses whether the vendor is in full compliance with specific requirements of applicable regulations. This assessment can serve as a common basis for doing business.

Organizations attempting to manage their vendors' privacy compliance using manual processes quickly realize it is prohibitively costly and inefficient. Especially with a largely remote workforce, a centralized privacy assessment platform, accessible from anywhere, enables privacy officers, information security teams, outside counsel and clients to collaborate in the delivery of the assessment and simplifies reporting. More sophisticated platforms will allow larger enterprises to assess and compare the readiness of internal business units or departments as well as integrate with a host of digital privacy tools.

The journey toward data privacy compliance requires significant shifts internally and externally, demanding demonstrable governance and accountability. Successful implementations of vendor management for the CCPA or GDPR call for proper executive support, stakeholder engagement, documentation management and careful tracking.

Rich Vestuto *is a managing director at Duff & Phelps, where he leads the firm's information governance, records and contract management capabilities, leveraging his over 20 years of experience in contract lifecycle management (CLM), information governance and eDiscovery supporting complex litigation, M&A and regulatory engagements.*

Wayne Matus *is the co-founder and general counsel at SafeGuard Privacy. His extensive law firm and in-house experience in litigation, investigations, privacy, compliance and information governance, enables him to solve eDiscovery, privacy and data-related problems for large and small organizations.*