Managing the Challenges with Burgeoning Data Privacy Laws

August 2020

PREPARED BY: SIG & TAILOR RESEARCH

How are data privacy laws shaping businesses today, both globally and in the United States? As different data privacy laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) emerge, we gathered insights into the complex interactions between legislation and vendor management, particularly as they pertain to vendor relationships, suppliers, and contractors.

To gain perspective on these data privacy regulations, we interviewed four procurement veterans, asking about their experiences with these laws. We distilled data privacy laws and the interview findings into this study to address the intersection between data privacy and vendor management practices.

Important Data Privacy Laws

GDPR is probably the best-known data privacy legislation. A landmark piece of law, it is widely considered to be the most important data protection regulation change in 20 years. The GDPR went into effect on May 15th, 2018. All companies processing and holding the personal data of subjects residing in the European Union (EU) must comply with it, regardless of location.

The CCPA is the latest in a series of laws that prompts companies around the world to reexamine the way they do business. Like the GDPR, CCPA is concerned with digital privacy rights; it impacts businesses that work with personal data.

CCPA applies to any for-profit enterprise that does business in California above a certain scale. Businesses are required to comply with CCPA if they have annual gross revenues of more than $25 million, earn more than half of their revenue by selling personal data, or possess personal data from at least 50,000 consumers or households.

CCPA can apply to entities doing businesses around the world; In fact, global businesses that are unaffected by the GDPR may still be impacted by CCPA, if they do business in California. CCPA applies to any entity that owns, is owned by, or shares common branding with a business covered by the legislation.

In addition, several other US states have also moved to enact data protection laws as well. Although CCPA is the best known, it is far from the only state-mandated law. Nevada's internet data privacy law (SB 220) went into effect on October 1st, 2019. The new data security requirements of New York's SHIELD Act became active on March 21st, 2020, and several other states have related legislation under consideration.

With all these laws emerging, managing data privacy risk has become increasingly challenging.

Data Privacy Compliance and Going Beyond

Data privacy laws impact virtually everyone, so businesses need to look beyond just CCPA and GDPR. Paulo, a third-party and procurement executive for compliance and risk management companies shared that although many people can say that they

Businesses are required to comply with CCPA if they have annual gross revenues of more than $25M, earn more than half of their revenue by selling personal data, or possess personal data from at least 50,000 consumers or households.

"Many people can say that they have heard of CCPA and GDPR, but they may not know all the various privacy laws that exist."
- Paulo, a procurement executive for an IT risk management company

have heard of CCPA and GDPR, they may not know all the various privacy laws that exist. Understanding suppliers and their unique data privacy risks beyond the recent regulations is essential.

Procurement professionals need to know how vendors collect and share personal data, both before and after data processing. They need both a clear understanding of their standard practices and a detailed grasp of what's in their vendor contracts. Finding and vetting vendors is an increasingly complex process, especially when companies are still using antiquated systems and procedures. Many procurement professionals still vet vendors using spreadsheets and questionnaires sent through email attachments; this needs to change. The process of selecting vendors and contracting their services should be far more sophisticated.

Organizations face 22 security breaches per year

Average cost per attack $380,000

- Accenture[1]

Pros of Embracing Data Privacy Laws and Cons of Not

Organizations need to be concerned about data privacy laws because security breaches are costly. According to Accenture[1], organizations face 22 security breaches per year on average, and the average cost per attack was $380,000.

However, compliance with data privacy laws can have a positive impact on an organization as well. According to Capgemini[2], 81% of proactive organizations stated that GDPR had a positive impact on the organization's reputation/brand image; 84% stated that trust increased, while 76% saw revenue increase.

"81% of proactive organizations stated that GDPR had a positive impact on the organization's reputation/brand image; 84% stated that trust increased, while 76% saw revenue increase."
- Capgemini[2]

According to Deloitte[3], 21% of Chief Procurement Officers (CPOs) stated that the technology area that will have the greatest impact on their business over the next two years is data privacy/cybersecurity.

The amount of money being spent on compliance grows with every new law. According to PWC[4], when organizations were preparing for GDPR to take effect in 2018, 77% of responding US multinationals expected to spend $1 million or more on GDPR compliance, 68% expected to invest between $1 million and $10 million and 9% expected to spend over $10 million to address GDPR obligations.

Which Industries Might Be Impacted Here?

Highly regulated industries, like healthcare and financial services, are more well prepared to face oversight in this area since they have always operated under strict regulations. On the other hand, industries that have historically been less regulated may struggle to adapt to this new level of scrutiny. The technology industry, for example, has generally operated with little regulation. Paulo, who came from the industry, described it as having very little risk assessment evaluations performed on vendors. He stated that there was very little vetting of vendors nor insight into vendors' processes.

Professional service providers may experience a steep learning curve as they come into compliance with CCPA and other data privacy laws. For example, legal and accounting firms are particularly vulnerable because they are frequent targets of cybercriminals. If hackers can gain access into their systems, they can get all their clients' most confidential data.

Professional service providers may experience a steep learning curve as they come into compliance with CCPA and other data privacy laws.

Key Strategies to Meet Data Privacy Regulatory Requirements

1. Conduct thorough due diligence and risk assessment, digitally.

Sophisticated risk professionals recommend giving prospective vendors a standardized questionnaire to fill out. This is a good way to learn how they use data, what kind of data they work with, and more broadly, whether they will expose your business to risk. You can streamline this process and speed it along by digitizing the questionnaire. Instead of giving your prospective vendors a long Excel form to fill out, DocuSign Guided Forms provide a step-by-step experience to help vendors easily complete long or complex forms with questions that adapt based on previous answers. The result is a faster, friendlier experience for vendors with fewer errors and less friction.

2. Identify risk areas across contracts.

Data privacy regulations impose requirements on businesses that share or sell personal data, including when the "sale" is not for traditional monetary gain. To address these

requirements, you need to know how your vendors collect and share data, both before and after your interactions—and that requires clear knowledge of what's in your contracts. The challenge is that contracts don't generally contain standardized terms around data privacy issues, so even a searchable contract repository won't obviate a tedious manual review effort.

Both Paulo and Alejandro (Global Vice President of Indirect Procurement at a global chemical and ingredients distributor) pointed out the importance of AI tools to help streamline the process. DocuSign Intelligent Insights uses AI-driven analysis to provide 360-degree visibility into agreements, regardless of how and where they are stored. Intelligent Insights also have a Data Privacy Insight Accelerator with prebuilt extraction packs to automatically detect relevant contract terms, with a conceptual understanding of your vendors' commitments around personal data use, enabling you to manage and mitigate data privacy risk where necessary.

3. Generate revised agreements with vendors that share data.

Once a company has identified the data privacy weak points within a vendor contract, they will want to amend and renegotiate contract terms. Traditionally, "repapering" agreements with vendors is a painstaking, costly, and error-prone process, as all of our interviewees pointed out. However, DocuSign CLM streamlines this process by automating contract creation, negotiation, and approval. Leveraging preapproved clause libraries allows you to make sure important data privacy language is included in agreements. DocuSign CLM helps you efficiently build contracts by leveraging previously approved clause language and source data from your enterprise systems. It also helps you shepherd vendor contracts through complex negotiations and proprietary workflows.

4. Execute revised vendor contracts quickly and efficiently with all signatories.

CCPA started penalty enforcement on July 1st, 2020. With other data privacy regulations looming, procurement contracts that have been revised for new data privacy laws need to be executed in an efficient, reliable, and legally binding way. It's becoming more important for businesses to keep detailed records of who has signed specific versions of the contracts and

when they were signed. DocuSign eSignature provides reliable enforceability of revised agreements with timestamped, tamper-evident, and court-admissible audit trails.

These key strategies, along with standardized language and best practice processes, will enable procurement professionals to avoid common pitfalls in their vendor contracts.

Using Standardized Language and Processes to Avoid Pitfalls

Pitfalls in data privacy protection can start at the contractual level. Sometimes companies omit important areas in a vendor contract. When a company neglects needed contractual steps, it can be difficult to recoup.

Al, an information privacy and security expert at a $2.5 billion financial services company, discussed his experiences with companies skipping steps and not using standardized language in contracts. He stated that it is essential to have standardized language in all contracts so a company is not left trying to "push the vendor to do something that is not already defined in the contract." He stated that the standardized language should include a set of expectations and obligations around security and data privacy.

It is essential to have standardized language in all contracts so a company is not left trying to "push the vendor to do something that is not already defined in the contract."

Process-Related Challenges

Many of the challenges involved in assessing data privacy risk can be described as process-related. The problems can usually be traced back to the start of the vendor relationship, and to a lack of clarity at the outset. Successful companies bypass this problem by putting a well-defined procedure in place which everyone is trained to follow.

Fortunately, the DocuSign Agreement Cloud makes it relatively easy to revise a contract securely, no matter when it is initially signed. DocuSign CLM automates the contract process, from creation through negotiation to the approval process. DocuSign Intelligent Insights uses AI to identify high-risk clauses and suggest preapproved language for revised terms. The result is a smoother, quicker renegotiation process.

Having a robust process in place is critical to the success of onboarding vendors, especially with data privacy issues.

Designing the process should be a collaborative effort among stakeholders including legal, security, risk and compliance.

The Vetting Process

The requirements of data privacy laws mean that businesses need to have greater visibility than ever before into their suppliers and contractors. Procurement professionals will need to conduct a far-reaching and thorough vetting of every vendor they do business with to ensure that they are processing data in accordance with the new requirements. Failing to properly vet means exposure to unexpected risk.

Data privacy laws mean that businesses need to have greater visibility than ever before into their suppliers and contractors.

The traditional approach to this process is a hands-on investigation, which is carried out in person by sending a team of assessors to go on-site to audit the vendor. The assessors can then go through the data center and offices to verify that all standards are met. This approach has its merits, but it is also problematic.

Troy, Head of Third-Party Risk for a Fortune 100 software company, stated that site audits can be very labor-intensive. He explained that it is expensive and difficult to have a team of company-employed assessors go on-site globally to verify that all standards are met. Plus, hands-on assessment may not be realistic in many cases because of the expense and labor involved, as well as restrictions on access imposed by vendors.

"Hands-on assessment may not be realistic in many cases because of the expense and labor involved, as well as restrictions on access imposed by vendors."
- Troy, Head of Third-Party Risk for a Fortune 100 software company

Effective Risk Assessment

Every business decision involves some level of risk exposure. With that in mind, risk assessment is a thorough examination of all contracts, agreements, and business dealings to identify which one of them may violate data privacy regulations. A successful risk assessment process will consider the specific, unique circumstances of each business relationship.

It's important to establish clear data definitions, data classifications, types of data, and ownership of data. Companies like Home Depot and Target were forced to learn this lesson the hard way when their systems were compromised by hackers gaining access to sensitive data via third-party vendors.

A thorough risk assessment should also incorporate a geographical risk assessment. During a pandemic such as

COVID-19, businesses have grown more conscious of the role that geography plays in the assessment.

Troy described geographical awareness as an important element in controlling the overall risk. He also stated that a company should have a geographical-based standard. For example, a company may not allow contracts to be signed for vendors that operate in countries with high-risk profiles. Similarly, vendors in countries with a moderate risk level may need a more thorough assessment than a country with a low-risk level. Assigning a risk profile to each country depends on many factors, but a company should develop overarching guidelines that address key considerations, such as country-specific infrastructure, laws and labor practices.

A successful risk assessment will include a study of the impact on supply chain business continuity

In addition, a successful risk assessment will include a study of the impact on supply chain business continuity. Broadly, this means making sure that data privacy considerations are included in vendor contracts. Specifically, it means evaluating the relationship with each vendor and determining whether there is higher versus lower dependency for that vendor. In cases with high dependency, prudence likely dictates testing every year, whether that is by conducting the test directly or requiring the test to be carried out by a third-party.

Determining business continuity also means assessing how stable each vendor is, and how well-prepared they are to face changes in the data privacy landscape. A good assessment will determine whether each vendor is able to continue to operate and provide their services in a timely and satisfactory manner, without being derailed by penalties for failing to comply with data privacy laws.

Risk Tiering

Most organizations already use a tiering system to assign each of their vendors a level of potential risk. Normally, this classification is carried out during the vendor onboarding process. The vendor is placed somewhere on a scale based on their risk assessment score, such as none, low, minor, moderate, high, and critical. The levels are determined based on a series of questions and, where applicable, an on-site investigation of the vendor's working practices.

The levels are determined based on a series of questions and, where applicable, an on-site investigation of the vendor's working practices.

Considering new data privacy legislations, risk tiering needs to be expanded to include the potential risks posed by

improper handling of personal data. A best practice here is to assign each vendor a score (comparable to a credit score or a cybersecurity score). This will likely be the first step in a larger process of assessing new vendors or updating data processing terms with existing vendors. Vendors with different risk tiers will receive different levels of scrutiny.

Most businesses will not engage vendors with a risk assessment score above a predetermined level. However, they may make an exception for firms that provide strategic value or uniqueness. A company should consider the broader business relationship with the vendor first and leverage risk score as a data point when evaluating the vendor.

Common Pain Points in the Vetting Process

We have examined some of the most common pitfalls that can plague the vetting process. But even the smoothest, most carefully managed process tends to run into pain points. Some of the most common ones are the legal review process, tight timelines, and business priorities that govern the process.

Fortunately, these are both areas where DocuSign eSignature can make an enormous difference. When procurement professionals finish negotiating with a supplier and are ready to move forward with the contract, they don't need to waste valuable time arranging a face-to-face meeting. All parties involved will be able to sign the contract from any location on any device.

Another common pain point is the slow process of waiting for responses when collaborating on a document with other parties. It can be frustrating to wait days or weeks for someone to pay attention to the changes and respond to them. Alejandro, a global procurement executive at a chemical company, stated that having the ability to configure and use AI to get straight into the redlining process would be very helpful. DocuSign provides the workflow automation necessary to support and automate redlining. This means that procurement teams are not stuck manually sifting through their messages to see whether colleagues have responded to their suggestions. Instead, the process is automatic, smooth, and centralized.

DocuSign eSignature

DocuSign provides the workflow automation necessary to support and automate redlining. This means that procurement teams are not stuck manually sifting through their messages to see whether colleagues have responded to their suggestions. Instead, the process is automatic, smooth, and centralized.

Conclusion

While complying with data privacy laws can be multi-faceted, time-consuming, and even expensive, the alternative is far less desirable. As data privacy executives pointed out, a methodical approach to data privacy compliance is essential. This new strategy involves getting to know vendors from various angles (their data privacy programs, their technology, their geographical location) and having sophisticated systems that enable procurement executives to mitigate risks.

Not all vendors need the same level of risk assessment resources, so risk tiering should be the first step to build flexibility into your program. Involving input from different stakeholders to ultimately reach sound risk mitigation decisions is what our interviewees repeatedly suggested.

Interviewee Profiles

Troy

Former VP and Head of Third-Party Risk at a large regional bank and one of the largest global software companies

Troy built and ran a broad supplier relationship management program, which included risk as one of the four pillars. He's run many third-party risk management programs, as well as FDIC and FRB program remediations regarding third-party risk management.

Paulo

Head of Third-Party Risk, Vendor Management, Governance, Compliance, Enterprise Risk Management and Strategic Sourcing at an information technology risk management solution company

Paulo implemented a global vendor risk program, supporting the vendor lifecycle process, including contract and risk assessment reviews. He designed and executed vendor training programs that focus on areas such as trust, security, and compliance while developing detailed assessment requirements for suppliers, which included AML and OFAC evaluation criteria. Paulo also created a company-wide vendor engagement process and intake system, developed risk classification methodologies, implemented vendor risk management software and created an intake process to determine the level of due diligence required.

Al

Information Privacy and Security Expert consulting clients in the financial services, technology, and health industries

Al established and managed data privacy programs, including processes such as Privacy by Design (PbD), data inventory, DSAR, privacy impact assessments (PIA), and Vendor Privacy Risk Management. He has led and successfully completed the CCPA compliance project by developing and implementing processes and procedures to meet its requirements. He's also

conducted PIAs of various products and business processes, documented findings, and recommended remediation where applicable.

Alejandro

Global Vice President, Indirect Procurement at a $9 billion global chemical and ingredients distributor

Alejandro is a member of the Procurement Leadership Team charged with the procurement strategy and category management for Capital and MRO categories. He also has functional responsibility for all procurement activities for the South America region. Previously, he led all the strategic sourcing initiatives for professional services at a publishing company.

Citations

1. Accenture Third Annual State of Cyber Resilience Report
   Pages 9, 13
2. Capgemini Championing Data Protection and Privacy Report
   Page 17
3. Deloitte Global Chief Procurement Officer Survey
   Page 30
4. PwC GDPR Readiness Survey