DocuSign®

Whitepaper

Four Strategies for Data Privacy Law Readiness

Regulation around data privacy is a complex patchwork of different international, national and local laws that makes compliance increasingly difficult. The passage of General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the U.S. have given data subjects new rights and fundamentally redefined the relationships between businesses and consumers. On the heels of those laws, new regulations are being proposed all over the world that will give consumers new rights over their personal data.

As additional laws are passed and become enforceable, businesses have to establish new processes to responsibly manage customer data and meet their obligations under evolving privacy regulations. There's no singular path to achieve compliance with the existing series of laws, let alone remain compliant with the complications introduced by future laws and amendments. Instead, businesses need to focus on individual compliance workflows and strategies that will streamline necessary actions.

In this ebook, we'll examine four critical data privacy strategies. For each one, we'll dive into the most important topics to consider and how modern technology can facilitate compliance efforts.

Step 1
Analyze data privacy risk areas across agreements

Agreements evolve over time. Any time there's new regulation that impacts data rights, it's important for organizations to dive into existing agreements and see how the language stands up in light of the new guidelines. When legislation changes privacy laws on a broad scale – like GDPR or CCPA – businesses need to examine existing language and use that new lens to define relationships with any relevant party: customers, regulators, vendors, partners, employees and more.

As those agreements are analyzed, there's a series of new questions to ask. Are the terms of existing relationships still compliant? Are there now gaps in the agreements? Is any party obligated to take action as a result of the new law? If so, what's the timeline for taking that action? Here's a quick rundown of some areas of interest that are particularly relevant to analyzing agreements regarding data privacy:

Classifications/restrictions around service providers

At the heart of CCPA is a reclassification of all organizations into three categories: businesses, service providers and third parties. To begin understanding obligations and responsibilities, organizations need to clearly identify the correct role for each party in its library of existing agreements. This is true beyond just CCPA. Successful agreements will clearly identify roles and relationships of every party involved. Once that analysis has been done, there needs to be additional clarification around what services are provided and the restrictions/obligations for each party to ensure those services are delivered correctly.

Transparency/audit rights

An important part of business-to-business relationships is diligence research before an agreement is signed. It's imperative that an organization put privacy and security information front and center so other companies and customers can find it easily. Moving forward, new agreements will require audit provisions to review vendor relationships on an ongoing basis to make sure that every party is fulfilling their obligations.

Security breach provisions

During agreement analysis, organizations need to clarify details about what happens in the event of a security breach. No organization ever plans for a data breach, but they still happen and making mistakes in a post-breach response only compounds the error. There are a series of different laws that are a part of this process (especially if business is done in multiple states or countries), and compliance failures result in large fines, so it's important to have this process thoroughly defined in paperwork. Proper agreements will specify the obligations of each party in the event of a breach, notification processes and how liability will be apportioned.

Arbitration clauses

An interesting development in business-to-consumer relationships is that companies have been including arbitration clauses in terms of service to avoid class action suits. Recently, the way that suits against companies are filed has changed, with multiple customers individually suing a company rather than a collective class action suit. That change has resulted in businesses owing millions of dollars in fees before arbitration even starts. To avoid those fees and unnecessary arbitration processes, businesses are including new language in agreements. CCPA appears to limit parties' ability to waive the right to a private action if consumers are affected by a data breach of certain types of personal information.

Widespread agreement analysis is manageable, but the issue is volume. Depending on the size of an organization and the nature of its work, it could have a base of tens of thousands of agreements that need to be analyzed. It's simply not reasonable to manually process all those documents to identify areas of impact. Even a keyword search can miss crucial risks and opportunities in that language.

How DocuSign can help

DocuSign Intelligent Insights is purpose-built to analyze enormous volumes of agreements. It starts by creating a central repository of searchable texts, using optical character recognition to combine documents from almost any source and file type into a single searchable library. From there, Intelligent Insights uses AI to scan the text and analyze language by broad concept rather than simple keywords. DocuSign even built a data privacy Insight Accelerator to analyze agreements for this specific use case. Intelligent Insights radically reduces analysis time by pinpointing and extracting exact agreement language about data privacy, company roles, customer protections in different geographies and liability, freeing up hundreds of hours of manual labor.

Step 2
Update agreements efficiently to adhere to applicable standards

After you've done agreement analysis and found language that needs to be updated, you need an efficient way to make those corrections. The first step here is to gather all of the agreements that require action, then determine which laws are applicable and what the updated agreements need to include. It's simply not scalable to make a series of one-off adjustments, there has to be an efficient process to make changes across a broad base of contracts. Here are a few important topics to consider at this stage:

How consistent are the changes you need to make?

As agreement analysis finds problematic language, teams need to understand the scope of work that needs to be done. Is the fix as simple as updating a single paragraph with a new clause and copying it across multiple agreements? Do agreements with businesses in different states require unique language? In a lot of cases, different data privacy laws are similar and compliance can be managed with across-the-board updates, however there are security requirements, use restrictions, breach directives, etc. that have to be considered.

New addenda vs. new templates

In most cases, the simplest solution to new data privacy language is to update companywide agreement templates. However, there will still be some specific cases (for example, highly regulated fields like financial data or healthcare data) that will require separate addenda. Businesses need to analyze the frequency of those cases and make a decision about which templates and addenda to prepare for widespread usage. It might be tempting to insert a blanket statement that a company "agrees to comply with all applicable laws," but these statements can be extremely risky as new laws are added. In general, businesses need to include provisions to demonstrate that they understand specific data privacy obligations.

The value of prepopulating data

Any time new data is entered into an agreement, the process introduces room for delays and errors. To help with this, businesses rely on integrations that can automatically pull data quickly and accurately. If the same information is consistent across multiple agreements, a single data pull can guarantee consistency and efficiency. As information from additional systems is included in agreements, the value of prepopulating data increases exponentially.

The importance of change management

A new law that requires updating existing agreements and templates can also be an opportunity to update other language in those contracts. Changes that start out simple can result in a list of agreement updates too long for a team to handle. To manage these changes appropriately, it can be helpful to sort agreements into tiers – starting with a Tier 1 – of contracts that are most sensitive to address immediately and moving down to less pressing updates.

How DocuSign can help

DocuSign CLM is a tool specifically built to make smoother transitions in document workflows. As contracts are generated, they can be automatically populated with relevant data. The process to approve these updates is also far simpler due to increased visibility into redlining, version control and next steps in the workflow. With every step of every agreement connected in a single place, the legal team can create a library or preapproved clauses that can be included in any contract that needs updating.

Step 3
Capture consumer consent to changing terms and conditions

Focusing specifically on business-to-consumer relationships, it's becoming increasingly important for companies to manage customer consent. As new laws grant customers more power over their data, it's vital to make appropriate updates to terms and conditions to ensure customers are informed of their rights and give the business permission to collect data. Below are a few important topics to consider regarding consumer consent:

Ensuring adequate disclosures

With GDPR, CCPA and other laws that detail the handling of customer information, companies have a few important responsibilities. The first is to change how the business operates to comply with new regulations. The second is to disclose those changes so customers understand their rights and how to take action on their data. Finally, a system needs to be set up that allows customers to easily acknowledge receipt of disclosed information and provide consent for their data to be collected.

Proving valid consent

Keeping accurate and easy-to-find records of customer consent will be necessary for compliance with data privacy laws, and will also be important for litigation purposes. Accurate records will be the easiest way to prove that a user agreed to an arbitration clause, updated terms of service or any processing activity (like using cookies). As soon as a customer provides consent, the action needs to be recorded accurately in case proof is required for any reason.

Variables across laws and jurisdictions

As data privacy laws evolve in a patchwork of regulations, there are cases where customer consent is needed and others where it is not. Depending on the specific obligations and regulations, companies need to be able to figure out different requirements quickly. Consent capture may be legally required or simply a company's preference, but it's vital to quickly determine when consent is needed. This is especially important as organizations react to local regulations that change over time.

How DocuSign can help

DocuSign Click is an easy way for any business to capture consent to agreement terms in an embedded experience with a click of a checkbox or buttons on a website or app. Click works side by side with DocuSign eSignature to capture acceptance of terms and conditions with a single click. It also logs information about which customers have agreed to which version of that agreement in case that information is needed for litigation or other purposes.

Step 4
Process data subject access requests securely and quickly

One of the new powers granted to consumers in GDPR, CCPA and similar data privacy laws is the right to access a copy of their data and optionally delete that data. To respond to consumers' data subject access requests, businesses need to implement operational changes to locate personal data quickly and deliver it securely. Responding to a data access request is nearly impossible if a company doesn't know where the information lives and doesn't have a workflow to accept and respond to these requests. These workflows need to be built on visibility, transparency and communication. Below are the important steps in the processing data requests:

Collecting the request clearly

To initiate the requests, consumers need a simple way to submit requests for their data. Depending on the complexity of the work done and the relationships with customers, a business may interact in varied ways with different types of data so these workflows need to be established correctly. Part of this intake process is making it clear to consumers exactly which information they need to provide to allow the business to process a request. Once the request is formally submitted, businesses need to be able to efficiently search across all systems to find data and fulfill a request for access, deletion, portability or any other action specified in data privacy legislation.

Confirming identity of the requestor

Likely the most resource-intensive step of fulfilling data subject access requests is verifying the identity of the requestor. To make things more complicated, there are a number of third-party companies that submit data requests on behalf of consumers. In those cases, the consumer's identity must still be verified, but additional verification must be done to ensure that the third party is acting appropriately on behalf of that consumer. Businesses that fail to verify identity correctly run the risk of giving data to the wrong party, which makes them liable for a data breach.

Ensuring delivery of data is secure

The end-to-end process from request to delivery needs to be secure at every step. After all the work to process a request and confirm a consumer's identity, if the data is not delivered in a secure way, a business can still be responsible for a data breach. Data requests often have well-defined delivery timelines, so it's important for businesses to maintain security as they move to get accurate data delivered quickly.

How DocuSign can help

DocuSign has a range of products to help with secure and efficient responses to data requests. DocuSign Guided Forms by SmartIQ are an easy way to streamline consumer submissions with step-by-step guidance on the request form and prepopulation of forms with data from other systems to reduce entry errors and time required to submit a form.

To assist with identity verification, DocuSign Identify offers a mobile-first verification experience that supports government photo IDs and European eIDs. Customers can choose from phone, SMS and knowledge-based authentication methods to support ID documents. There's also functionality to support parent/guardian validation as needed.

DocuSign eSignature is an established tool to collect signatures for the internal approvals that are part of requests dealing with personally identifiable information. With eSignature, encrypted data can be securely distributed, including certificates of completion, with every access point logged along the way in case it is necessary for an audit.

Simplify compliance with data privacy regulations

The DocuSign Agreement Cloud digitally transforms the way your business handles data privacy processes. The simplest way to analyze existing agreements for data privacy obligations, update contract language, capture consent and securely deliver consumer data is with modern agreement technology. DocuSign takes data privacy obligations to consumers seriously. As part of our commitment to empowering organizations to comply with customer data privacy laws, we ensure that we're also meeting the strictest privacy standards for our own customers.

World-class protection
Strong security mechanisms and robust operational processes allow DocuSign to meet or exceed the highest international security standards and protect documents and data

High availability
DocuSign eSignature maintains a scalable, high-performance, high-availability platform that provides continuous availability across the globe

Global reach and acceptance
DocuSign eSignature is lawful in most civil and common law jurisdictions for most agreement types and employed by hundreds of millions of users worldwide, including the European Union

DocuSign's first priority is to make your agreement experience safe and secure – and to ensure you have the information you need to feel comfortable transacting business online. Businesses around the globe rely upon the DocuSign Agreement Cloud for their most sensitive and time-critical transactions, and we're committed to maintaining the secure environment they've come to trust.

Learn more about the **DocuSign Agreement Cloud**.

DocuSign Agreement Cloud

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040

2020.08.18