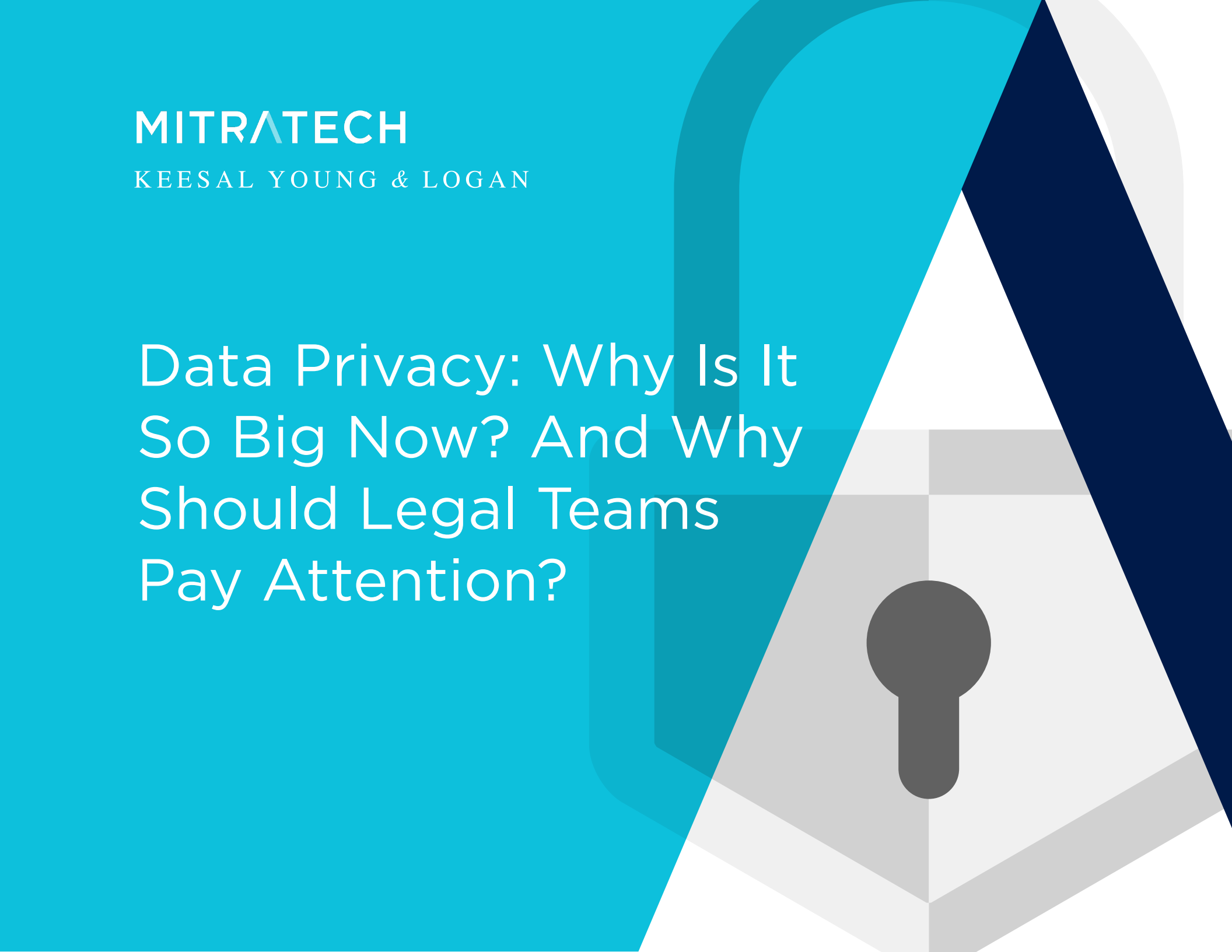
MITRATECH

KEESAL YOUNG & LOGAN

Data Privacy: Why Is It So Big Now? And Why Should Legal Teams Pay Attention?



Disclaimer This material has been prepared by Keesal, Young & Logan and Mitratech with information current as of August 5, 2019. This booklet is for informational purposes only and is not legal advice. Transmission of the information is not intended to create, and receipt does not constitute, an attorney-client relationship. You should not act upon this information without seeking professional counsel.

Table of Contents

01 Data Privacy: The Big Questions

The discovery of shady harvesting of personal data from unsuspecting internet users may no longer be news, but the shoe is continuing to drop in the form of government regulations.

Up until this point, the US has taken what might be characterized as a specialized approach to data privacy regulations. Rules and regulations have depended on the sector and industry where the information happens to be – for example, health information is governed by HIPAA, and financial information by the Gramm-Leach-Bliley Act. The US has dealt with privacy in a piecemeal fashion, with no laws in place that govern all private information, no matter who holds it, and in what context. This is in contrast with the EU's GDPR, which covers all personal data of individuals in the EU. In lieu of a federal regulation to cover the privacy of US citizens, states have started to take action on securing the rights of their citizens.

Data Privacy rules and regulations have depended on the sector and industry where the information happens to be.

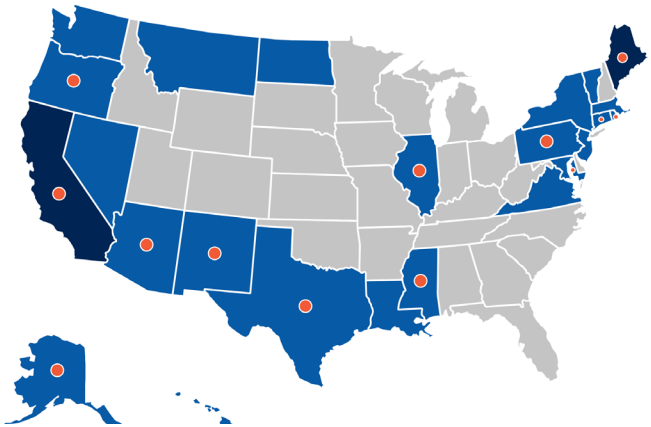
California has been the first state in the nation to enact a comprehensive privacy law, but companies across the US – whether they deal with California consumers or not – should pay attention to the wave of consumer privacy trends and demands for increased transparency on the horizon. California's act, which will be effective in January 2020, is only the foreshock of what will be a seismic shift to our data privacy landscape. Now is the time to prepare.

In this guide, our experts will bring you up to speed on the trends in data privacy. What businesses are obligated to comply with these new laws? And how should businesses prepare for the changes that lie ahead?"

02 What's the Context?

The CCPA focuses on giving consumers certain rights over their personal data, and also imposes obligations on certain businesses to recognize and implement those rights.

Because of the similarities between the CCPA and the GDPR, businesses that have prepared for the GDPR will have a head start. But the two acts aren't identical, so there are still steps to take. Not to mention, of course, that a number of states are following in California's footsteps. Thirteen states have enacted or are considering privacy bills modeled after the CCPA, and six states have proposed some degree of privacy regulation. So, let's dive into what makes a business subject to the CCPA.



- Enacted Privacy Laws
- CCPA Modeled Privacy Laws
- Pending Privacy Laws and Bills

03 Shaping Up by 2020

It's important for companies to recognize that not just Silicon Valley unicorns are obligated to the CCPA.

The CCPA is fairly broad in a number of different ways. But before we expand on the breadth of the Act, let's take a look at the general criteria that make businesses subject to the CCPA. A business must be a for-profit entity that does business in California, collects consumer personal information, and itself determines the purpose and means of processing the information. If a business fulfills these three criteria, it must also meet at least one of the following in order to be subject to the CCPA.

After a business hits those criteria, it must also have one of the following characteristics:

- Annual gross revenue of more than $25 million or...
- Annually buys, receives for a commercial purpose, sells, or shares for a commercial purpose, personal information of more than 50,000 consumers, households or devices; or...
- Derive more than 50% annual revenue from selling consumer personal information.

The CCPA does not require that a business have a physical presence in California. But California is the largest economy in the United States and the fifth largest in the world, so most companies with online sales deal with Californian consumers.

Even if only $1 million of a business's gross revenue is sourced from California and the rest elsewhere, that business arguably would still be subject to the CCPA. The information of 50,000 consumers would be collected if a company website had more than 137 hits per day. And deriving more than 50% of annual revenue from selling consumer personal information means that even small companies can be subject to the CCPA.

Personal Information is a broader term than one might think, and has been the subject of a great deal of commentary. It includes all information that identifies, relates to, describes or is capable of being described or linked with a particular consumer or household, and all inferences drawn from it. Personal information, as defined by the CCPA, includes the following (and all inferences that can be drawn from the following):

- Name and Alias
- Postal Address
- Email Address
- Social Security Number
- Account Numbers
- Driver's License Number
- Passport Number
- Telephone Number
- IP Address
- Physical Characteristics
- Religion, Ethnicity
- Commercial History
- Biometric Information
- Internet Activity
- Geolocation Data
- Audio, Visual, Olfactory, Information
- Education
- Profession or Employment

And what does it mean to sell personal information? This, too, is broader than one might expect. "Selling" means disclosing, making available, or transferring a consumer's personal information to another business or third party for monetary or other valuable consideration.

When businesses first determine whether or not they are subject to the

CCPA, it's a good idea for them also to take stock of all the states in which they do business. Rhode Island's proposed privacy law would apply to businesses that have more than $5 million in annual gross revenue; Pennsylvania, $10 million. Think of the CCPA as an opportunity to create a comprehensive approach to state privacy laws, or as an opportunity to create a system to handle each state in its own way. Either way, legals teams across the USA are an an inflection point.

When businesses first determine whether or not they are subject to the CCPA, it's a good idea for them also to take stock of all the states in which they do business.

04 Responding Strategically

So let's say you've met with your team and have determined that your business is a for-profit entity that does business in California, collects consumer personal information and has a gross revenue of over $25 million dollars, or you meet one of those other thresholds. What are you responsible for?

As individuals get more rights to control the use of their data, businesses must be prepared to be transparent about their practices and to follow through on certain requests to delete that data.

Here's the lay of the land:

Access

Businesses are required to disclose whether they are collecting PI, for what purpose, and with whom it is being shared.

What is it to you?

These disclosures must be made when or before data is shared, at which point companies must also tell their consumers what their rights are. If a company has a privacy policy, companies must include these disclosures within it.

How should businesses react?

- Accommodate newfound measures for transparency by updating privacy notices and policies with required disclosures about information collection and sharing practices.
- Update HR disclosures, processes and documentation.
- Update vendor / service provider processing agreements.

Disclosure

Under the CCPA, an individual will have the right to request that he or she receive the PI that a company has collected. Not only does that individual get to see his or her own information, but the individual also has the right to know whether and with whom that information has been shared.

What obligations does that create for a business?

Businesses must make available two or more methods for consumers to submit requests for disclosure of PI collected and PI sold: a toll-free telephone number and a website address, if the business maintains a website.

Company must respond to verifiable consumer requests.

While a "verifiable request" hasn't been completely defined yet, this generally means that the company will verify these requests through multi-factor authentication, passwords, and account information. The business must respond within 45 days, at which point it must respond in writing and provide the information in a readily usable format. The business must also let the customer know what personal information has been sold or shared for a business purpose.

A company must ensure that consumers have two or more methods by which they can request disclosure.

How should businesses react?

- Create channels for submission of verifiable consumer access and disclosure requests (toll-free telephone number and web page).

- Make sure that these requests are trackable and automated, so the business doesn't get lost in the weeds looking for the right information, or dinged for missing deadlines.

Do Not Sell

Under the CCPA, consumers have the right to opt out of the sale of PI have the right to opt out of the sale of PI to third parties. Businesses are required to have a clear and conspicuous link on the businesses' home page titled "Do Not Sell My Personal Information" that allows consumers to opt out of the sale of their personal information. Businesses must respect that decision for at least 12 months.

How should businesses react?

- Operationalize a "Do Not Sell My Personal Information" link on your website.

- Make sure that when an individual clicks on the link, the request is tracked, managed and fully auditable. Keep them on the workflow conveyer belt, and calendar follow-up for 12 months down the road. You'll want to take another look once the 12-month "opt out" period has passed.

Deletion

This aspect of the CCPA gives consumers the right to request that businesses delete personal information that the business has collected from the consumer. There are, however, a number of exceptions. Businesses are not required to delete personal information if they are required to keep that information to comply with legal obligations, to complete a transaction for which the PI was collected, to detect security incidents or fraudulent activity, and a number of other reasons.

How should businesses react?

- Create two or more designated methods for submitting requests for deletion, including, at a minimum, a toll-free telephone number and a web site (if the business maintains a web site).

- Ensure that deletion requests are routed appropriately and responded to in a timely and ideally automated manner.

Non-Discrimination

All consumers have the right to equal service and price, even if the consumer exercises his or her privacy rights.

How should businesses react?

Make it easy for customers to exercise their rights. Studies show that expertise and quick responses to data privacy concerns can elevate a business's reputation and enhance its relationship with consumers.

05 Getting a Head Start

Five Steps to Start

Before diving into specific solutions, businesses need to take inventory of where they currently stand and identify their data privacy strategy going forward. These five steps are a good start:

1. **Take inventory** of data collection and sharing practices.

2. **Identify** security gaps and update security measures.

3. **Define** the business's strategy for handling the CCPA and copycat acts: does the business plan to roll out a state-by-state specific strategy, or a comprehensive program?

4. **Educate** and train employees.

5. **Implement** consistent, repeatable, efficient protocols for authenticating and responding to access, deletion, and opt-out requests, including identifying overbroad and unfounded requests.

Keeping it Efficient (And Auditable) with Workflow Automation.

A workflow automation solution digitizes and automates repetitive processes, so businesses reduce or eliminate the "pain of the mundane" – high administration costs, errors, delays, compliance problems, even employee engagement issues – while accelerating process speed and boosting productivity.

The benefits of workflow automation have been recognized by the Association of Corporate Counsel. They write: "Manually responding to personal information access and deletion requests is likely to become overwhelming quickly. Organizations will need to implement an automated, streamlined approach."

"Manually responding to personal information access and deletion requests is likely to become overwhelming quickly. Organizations will need to implement an automated, streamlined approach."

Why Workflow Automation?

1. **Focus on what matters.** Focus on what matters. Automatically validate and verify requests for disclosure by asking consumers the right questions, and validating them with two-factor authentication or account information.

2. **Improve security and compliance.** Automatically record and audit all actions within a workflow, safeguard vital data, restrict access and roles of users and alert respective owners when any problems arise.

3. **Flexibility for the Future.** With easy-to-use drag-and-drop design tools, your workflows can be modified quickly and easily to account for changes in law or process.

4. **Centralize documents and access.** With manual workflows, there's no such thing as a centralized document database. However, with a single, unified database, your documents, forms, workflow records and other assets are readily available and never lost.

5. **Keep it on-brand.** Ensure that every communication with a customer is

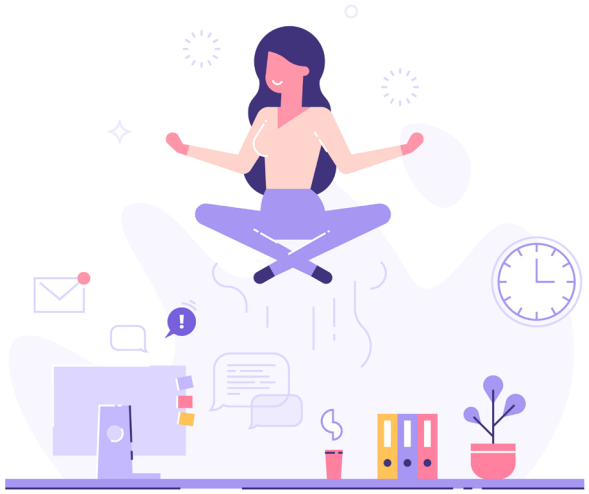
With an easy-to-use drag-and-drop design tools, your workflows can be modified quickly and easily to account for changes in law or process.

on-brand by templatizing responses and automatically ensuring that the consumer has an easy, hassle-free, and company-feel experience.

6. **Drive teamwork and morale.** A good workflow solution removes barriers to collaboration across teams and departments. By driving efficiencies so your team spends less time on manual tasks and more time on their actual jobs, you'll drive productivity, value and inspire happier employees.

What does a good workflow automation platform look like?

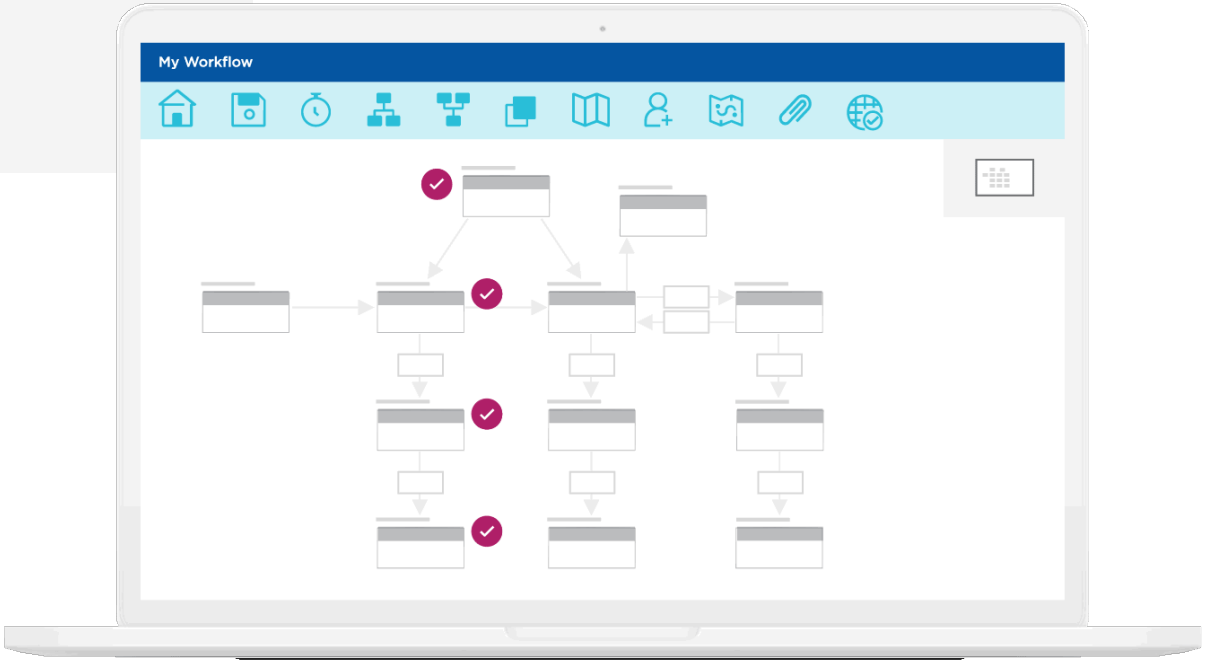
- Stringent security measures; only the right people with the right permissions should have access to view, access or copy certain documents.
- Workflows should be publishable to a public webpage, and as such branded for the public to use.
- Guided form experience; policy, procedure, and training should be baked into the form such that the user is asked only relevant questions and is sheparded down the easiest, most hassle-free path.
- Automatic and conditional routing; workflows should automatically triage requests based on if this, then that logic.
- Captcha fields and two-factor authentication; ensure that all requests are verified before sinking your lawyer's time.
- Time based escalations: If you have 45 days to respond to a request, make sure that, if there is no response by day 44, the workflow automatically requests an extension.



TAP Workflow Automation

Mitratech's TAP Workflow Automation empowers our customers to automate nearly any repetitive manual legal or compliance process, including data privacy workflows. TAP enhances agility and responsiveness, improves performance and compliance, and accelerates ROI, while also laying a reliable foundation for digital transformation and innovation across the entire enterprise.

Learn more here.



About **Mitratech**

Mitratech is a proven global technology partner for corporate legal professionals who seek out and maximize opportunities to raise productivity, control expense, and mitigate risk by deepening organizational alignment, increasing visibility, and spurring collaboration across the enterprise.

With Mitratech's proven portfolio of end-to-end solutions, operational best practices permeate the enterprise, standardizing processes and accelerating time-to-value. By unlocking every opportunity to drive progress and improve outcomes, we're helping legal teams rise to the challenge of serving the evolving needs of the modern, dynamic enterprise.

For more info, visit: **www.mitratech.com**

MITRATECH

CONTACT US

info@mitratech.com
www.mitratech.com

Mitratech US
+1 (512) 382.7322

Mitratech EMEA
+44 (0) 1628.600.900

Mitratech AUS
+61 (0)3.9521.7077

About **Keesal, Young & Logan**

The lawyers and security professionals at Keesal, Young & Logan (KYL) help companies evaluate their data collection practices and develop strategies and processes to comply with applicable federal and state privacy laws, including the California Consumer Privacy Act, the California Online Privacy Protection Act, the Gramm-Leach-Bliley Act, the European Union's General Data Protection Regulation (GDPR) and other state and federal privacy and security laws and regulations. KYL lawyers provide solutions that are both legally sound and commercially practical. KYL also defends clients who have been accused of violating various privacy laws.

KYL's deep bench of privacy and data security experts includes members with the following certifications: IAPP Certified Information Privacy Professionals in United States privacy law (CIPP/US), European privacy law (CIPP/E), privacy management (CIPM), and privacy technology (CIPT), Certified Ethical Hacker, ISO27001 CIS F, BARBRI Cybint Solutions' "Cyber Protection," "Cyber Intelligence," and OneTrust Certified Privacy Management Professional.

Learn more at www.kyl.com.

KEESAL, YOUNG & LOGAN

CONTACT US

KYL
info@kyl.com
+1 (562) 436-2000