MITRATECH

7 Steps To Take Toward Data Privacy Compliance

Learn the key measures in creating a flexible, defensible compliance framework within your enterprise.

Table of Contents

Introduction

Consumer data privacy is a global issue. Laws surrounding businesses' responsibilities with regard to consumers' rights around their personal information are becoming more common, creating a host of new challenges for compliance professionals.

Consumer concerns are justified. According to Risk Based Security, by Q3 2019 there had been 5,183 data breaches exposing 7.9 billion records, already surpassing 2018's total for that entire year.

In 2018, the European Union's General Data Protection Regulation (GDPR) set out the framework for the California Consumer Privacy Act (CCPA), the strictest law on data collection and processing to date in the U.S. This law, effective January 1, 2020, takes a giant step towards putting consumers in the driver's seat when it comes to data privacy.

The lessons learned from the GDPR and recent data breaches have revealed that manual processes and incomplete systems of record-keeping can't meet the complexities of todays' compliance demands. Businesses need a solid framework in place, and the agility to easily navigate the continually shifting twists and turns of consumer data privacy protection.

The lessons learned from the GDPR and recent data breaches have revealed that manual processes and incomplete systems of record-keeping can't meet the complexities of todays' compliance demands.

Compliance and accountability for not upholding consumer protections are already being enforced in the case of the GDPR, with mounting fines and injury to company reputations. From its inception to near the end of 2019, for example, nearly €360,000,000 in fines had been assessed by EU regulators.

More regulation in more places

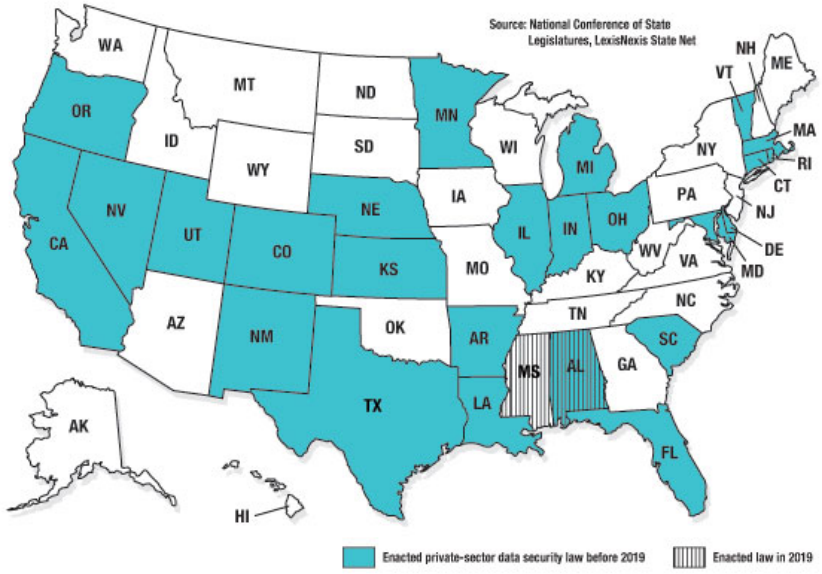
From 2017 to mid-2019, the number of countries that had enacted data privacy laws **rose from 120 to 132**, a 10% increase. Their data privacy laws usually covered both the private and public sectors, and **at least 28 other countries** had bills in various stages of progress. [1]

In the United States, **27 states** had enacted or were contemplating data privacy regulation in the absence of a unifying federal law. [2]

With these many different laws, compliance can become confusing, especially when counting up all the jurisdictions where your company does business.

[1] Greenleaf, Graham, Global Data Privacy Laws 2019: 132 National Laws & Many Bills (February 8, 2019). (2019) 157 Privacy Laws & Business International Report, 14-18.

[2] https://adage.com/article/news/how-brands-are-preparing-californias-privacy-act-becomes-reality-2020/2205586



Source: National Conference of State Legislatures

The steps to take toward data privacy compliance

To effectively manage compliance risk, legal and compliance leaders need to install a coherent, cohesive, and comprehensive approach to data privacy compliance with the many new statutes and regulations just described. Following are **the steps you should take immediately** to structure and manage just such a compliance framework.

In 2018, more than 6,500 data breaches were reported, exposing 5 billion records.

[3] https://www.darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875

01 Identify your risks, obligations, and the scope of your data

Determine your obligations under current law, including state and federal laws where you operate and recognize industry standards that require more specific analysis. Identify all the data risks within your organization including employees, vendors and third-party data.

Pinpoint technological and physical security threats for both internal and external audiences. Distinguish your data's jurisdiction by identifying where the data is stored and where it is accessed from. With this information, perform a gap analysis on how your current system stacks up. The gap analysis will provide you and your organization a strong business case for compliance.

Legal teams are recognizing that the legacy/homegrown or manual systems they've been using present a serious roadblock to smooth operations,

The risks aren't always intentional

Even in the best-intentioned organization, there can be data risks. Here, for instance, are some of the most common causes of data breaches:

- **Unpatched security vulnerabilities**
- **Human error**
- **Too many permissions**
- **Malware**
- **Deliberate insider misuse**
- **Theft of a data-carrying device**

The latter three are (obviously) malicious - but the first three can happen even if you're taking measures to protect yourself against outside threats and attacks. So understanding risks, obligations, and the total scope of your data is absolutely vital.

In 2019, 53% of global internet users had some degree of concern about their online privacy. [4]

[4] https://www.statista.com/statistics/373338/global-opinion-concern-online-privacy/

02 Choose a framework

To be compliant in today's marketplace? Your business has to be able to plan, prioritize and act on a wide variety of issues across your organization. So you should adopt a compliance framework that allows your business to comprehensively address your compliance needs. One that provides an understanding of all your data privacy obligations and risks, with the ability to report and respond quickly with ease.

Your controls and processes can become very intricate, which reinforces the need for a firm framework. There's rarely the need to start from scratch when it comes to the actual data-privacy standards it follows as there are international and industry guidelines like ISO19600 available to adopt to steer best practices.

This framework, and the tools you install beneath it, will allow you to proactively manage, streamline, automate and accelerate how you manage data, enforce policies, and will **save you time and money** in the future – because the need for strong data governance and management will just keep growing.

Make certain it's flexible and adaptable

With the rise of our connected society and the advent of the Internet of Things, the volume of data will keep snowballing with incredible speed. Already, it's estimated there are **2.5 quintillion bytes of data created *each day*** at our current pace.

A flexible data governance and compliance framework can provide a structure to manage it all. Without such a framework, organizations are more likely to treat their data haphazardly, developing policies around such issues as data privacy and data security **reactively and randomly**, rather than proactively in a systematic fashion.

You might even consider such a framework for an *insurance policy*, helping companies mitigate any risk that might arise from their data and reducing liability.

Avoid creating your own framework or standards, if possible, or the technologies you adopt. Choose a framework and tools that automatically update with emerging compliance requirements.

Already, it's estimated there are **2.5 quintillion bytes of data created *each day*** at our current pace.

03 Get C-suite buy-in

Protection from the costs of non-compliance – which can be **3 times higher** than the costs of a sound compliance program – is a great place to start to build a case for adopting a comprehensive framework. Stressing the need for a scalable solution to empower, manage, and streamline the complexities of corporate compliance obligations can be supported with a gap analysis and risk assessment.

Data security and compliance must become an integral part of your corporate culture. To that end, **leadership support and advocacy** is essential in ensuring success. Focusing from the top on this issue will not only communicate its importance to employees, but it'll provide consumers the reassurance they're looking for making a choice between you and competitors.

Leadership support and advocacy is essential in ensuring success.

This is another aspect of compliance that will help with sell-in to the C-suite: Not only does a comprehensive data security and compliance framework make sense in the regulatory arena, it can play an important role with your brand.

As consumers become more aware of how data is collected, processed and sold, many marketers know that having a strong consumer privacy stance can only strengthen their brands. Plus, taking the right measures to ensure data privacy can **prevent the reputational damage** that's impacted many companies who have suffered breaches.

04 Assign responsibilities and develop policies and procedures

Finding the right place to assign responsibility for corporate compliance within your organization may be challenging. Each enterprise will need to structure responsibility differently based on its industry or markets.

Typically, responsibility falls between Compliance/Ethics, Legal, IT or HR. Whatever the case, it's important that there's **clear ownership** of your corporate compliance efforts. Providing the essential resources to produce clear and agreed-upon outcomes will help assure a successful program.

All employees should know and understand the basic laws regulating data privacy, as well as their own responsibility for ensuring privacy compliance. As well as knowing what to do when there's a breach.

All employees should know and understand the basic laws regulating data privacy, as well as their own responsibility for ensuring privacy compliance.

Developing policies that address requirements in your industry and within your company can be addressed in five stages.

Stage 1: Establishing policy requirements

Stage 2: Drafting policies

Stage 3: Communicating policies and procedures

Stage 4: Testing understanding and affirming acceptance

Stage 5: Auditing policies for effectiveness and compliance

A policy should leave both parties in no doubt as to what their obligations and expected behaviors are, which should dramatically reduce the likelihood of a compliance breach.

State your compliance case

As enterprises grow, **policies and procedures play a key role** in maintaining their culture. In a similar way that policies influence culture, a company's goals permeate the organization. Well-drafted and effectively deployed policies can have an extremely positive impact on culture.

With input from leadership, develop a **privacy policy and brand statement** that includes assurances that the data protection principles have been respected. Having a strong statement as part of your corporate values will only reinforce its importance within the organization. Strong policy statements also build employee trust and pride in your brand...so leadership needs to communicate consistently and often on the importance of compliance to really reach and influence employees.

Automate policy management

Also? You should **capture and archive** accurate, time-stamped information on policy adoption, deployment, and response, and be able to quickly generate analytics and reports around it. This calls for a tech solution so you can quickly gauge how policies have been accepted and understood, or how effective the organization has been at meeting consumer inquiries and requests.

Without these insights, a compliance team faces an almost impossible task in proving it's making progress, or in identifying issues to be addressed.

55% of U.S. consumers say companies should have the primary responsibility for the security of their customers' online and mobile accounts, while 44% believe account owners should be responsible. Just 1% think the government should bear the onus. [5]

[5] https://secureswissdata.com/americans-worried-about-privacy/

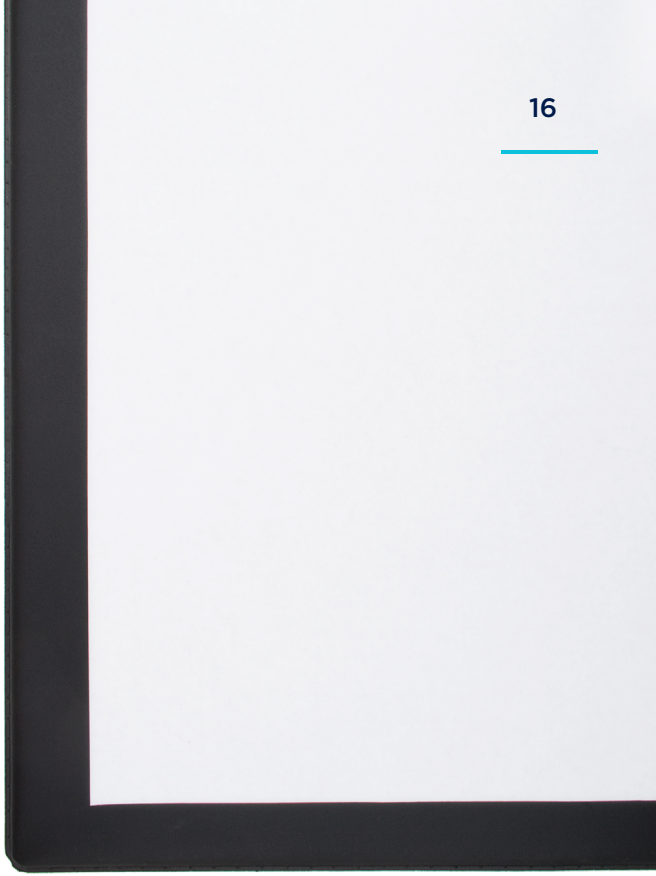
05 Build *defensible* compliance

It's not enough to build a compliance program. It has to be **defensible** under the scrutiny of regulators and the courts. To start, conduct the data inventory we mentioned earlier to identify the data your enterprise holds, where it's stored, how it's collected, used, and the retention policies in place.

As we said in the last section, having clear and well-communicated data management policies in place is a key factor in defensibility. As leading GRC pundit Michael Rasmussen wrote,

> *"To defend itself, the organization must be able to show a detailed history of what policy was in effect, how it was communicated, who read it, who was trained on it, who attested to it, what exceptions were granted, and how policy violation and resolution was monitored and managed."* [6]

[6] http://grc2020.com/2018/03/14/how-to-purchase-policy-training-management-platforms/



Knowing what data you possess and how it's protected can limit the potential for breaches, and saves considerable time and cost in any disclosure process, including when responding to Data Subject Access Requests (DSARs) which (confusingly!) are referred to as Verifiable Consumer Requests (VCRs) in CCPA argot.

Prove your responsiveness

Regardless of what they're called, you should be able to prove how responses to these requests are provided without delay. The GDPR and CCPA, for instance, **impose escalating penalties** for delays or failures in that process.

Be aware that the CCPA and the GDPR require notification of privacy practices prior to or at the time of data collection, as well as whenever there are any changes to your privacy practices. Consumers can request visibility into what data any given business holds on them, as well as how it's been shared, with whom, and they can also request to be forgotten (have their data scrubbed from your records).

Be sure to be current and compliant in all methods and touchpoints for data collection where consent is needed, and maintain an audit trail of all your actions. Show you're making consent easy to understand, and demonstrate to consumers and regulators like how you're acting in the spirit of empowering consumer data rights.

In 2019, the financial services industry was responsible for 62% of exposed data, though it accounted for only 6.5% of data breaches.

Source: Bitglass 2019 Financial Breach Report

06 Adopt empowering technology

Modern compliance demands are, as we've said, becoming increasingly complex, and the requirements and responsiveness demanded by regulations like the GDPR and CCPA allow no room for error. Even though "compliance" may involve handling thousands or tens of thousands of consumer requests for data access, deletion, transfer, or more.

Manual systems that rely on email and spreadsheets to ensure compliance simply can't keep pace. In fact, **they're a danger to your business** due to the risks they create. Successful data privacy compliance demands robust, adaptable, and – importantly – easy-to-use technology architecture.

The right solution enables the enterprise to effectively manage a data privacy policy and relevant documents and data everywhere within the organization. So compliance managers can document, communicate, report, and monitor all communications, training, tasks, responsibilities, and workflows.

Manual systems that rely on email and spreadsheets to ensure compliance simply can't keep pace - in fact, they're a danger to your business.

What's key here is to make sure you've defined your processes and requirements *before* purchasing new technology, or you run the risk of deploying the wrong product.

Some of the various technologies that companies consider - and the pros (and cons) of each:

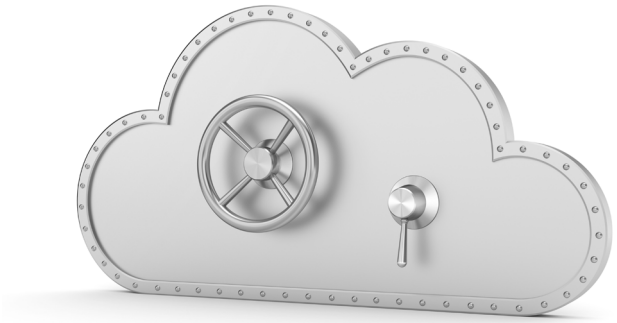
- **Email, spreadsheets, and documents software:** These are the traditional tools for conducting risk management-related processes, but they generate huge amounts of poorly organized information that consumes a nearly equal amount of resources to track and maintain.

- **Policy management solutions:** These can automate policy publication, distribution, and attestation, vastly streamlining the process of communicating data privacy policies to the organization and tracking employee or even vendor compliance. The best of them also securely archive your policy management processes for later audit, provide solid analytics and reporting, and are increasingly easy to use for admins and employees alike – an important point in ensuring adoption and internal compliance.

- **Workflow automation:** By digitizing and standardizing the processes involved in data privacy compliance – such as response to consumer requests, or internal data audits – an enterprise can elevate the accuracy of these processes while cutting the costs and labor required. The best of these solutions also can integrate smoothly with other tools, like databases or policy management software, to drive efficiencies and reduce errors across the organization.

- **Consent solutions:** For companies with multiple websites or other digital touchpoints, being able to display up-to-date opt-in messages (for GDPR compliance), or ensuring other online compliance measures are met in a variety of markets with varying rules has driven the growth of digital consent solutions and platforms that manage consent across all these sites and jurisdictions.

- **Enterprise content management (ECM) solutions:** The great amount of documentation and content created in many companies, especially in highly regulated sectors like healthcare and financial services, demands tools capable of centrally storing and controlling it all in a compliant way. An ECM solution can drive data privacy compliance by allowing easy collation of an individuals data when requested and ensuring accurate execution of their “right to be forgotten,” among other tasks.



07 Plan for monitoring, analytics, and reporting

Monitoring and reporting the status of data privacy obligations is an absolute necessity, and should be conducted with tools that allow reporting and analysis in as close to real-time as possible.

You have to understand your **maturity level as an organization** when it comes to your monitoring and reporting processes, first and foremost. Only then can you conduct proper risk assessment around data privacy compliance, and have the information in hand that regulators will want to see if they come knocking with an audit or accusation.

Mastering monitoring, reporting, and analytics gives you the opportunity to spot trouble before it happens so you can mitigate risk, and fine-tune compliance processes to eliminate errors and exposure.

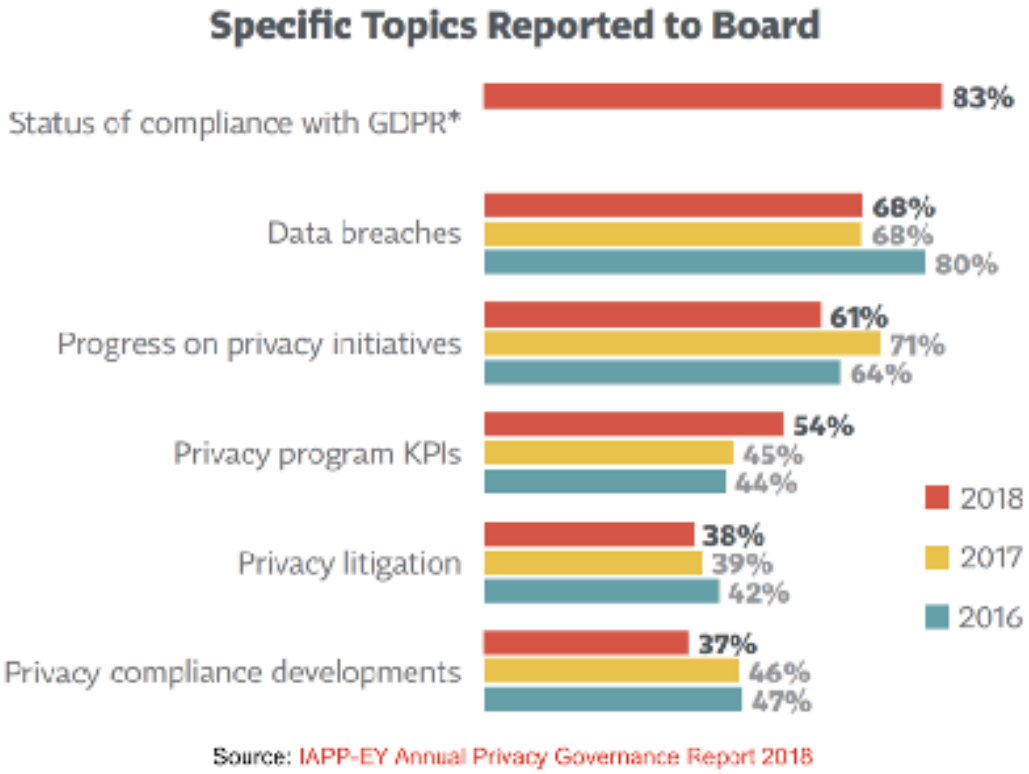
Mastering monitoring, reporting, and analytics gives you the opportunity to spot trouble before it happens.

Accountability is a broadening concern

Another reason for having a good monitoring/reporting mechanism in place? Data privacy compliance is very much **a concern of the C-suite and Board of Directors** these days.

This is due in part to their traditional responsibilities in stewarding a company. Another contributing factor? There's an increasing public and regulatory expectation of **personal accountability** on the part of directors, officers, and senior management. Now, both the organization and the people leading it may be found liable for data privacy violations.

Take note of this example of the many GDPR-related topics reported to company boards during the first year of the law's implementation. Similar situations are, no doubt, underway presently as CCPA and other statutes loom:



Notifications and alerts

Companies who rely on manual processes for monitoring and reporting on data privacy are lagging the field when it comes to addressing issues like data breaches. They may do diligent data discovery, but in the event of a breach there are inadequate procedures in place to **help prioritize risk to inform key personnel in a timely way** so they can act accordingly.

Automating the notification process with tools like integrated workflow automation can make a tremendous difference in identifying problems before they occur, or at least reacting to them ASAP.

About Mitratech

Mitratech is a proven global technology partner for corporate legal, risk, and compliance professionals seeking to maximize 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 spread throughout the enterprise, standardizing processes and accelerating time-to-value. By unlocking every opportunity to drive progress and improve outcomes, we're helping legal and GRC 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

We can help you meet your legal and compliance technology demands *today*.

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