Compliance Management Software for Total Data Privacy

The End-to-End Solution for Enterprise Compliance Management

The EU's General Data Protection Regulation (GDPR) went into effect on May 25, 2018. The January 1, 2020 deadline for the California Consumer Privacy Act (CCPA) had barely passed when its successor—the California Privacy Rights Act (CPRA)—was signed into law. Data privacy regulations such as these have ushered in a new era in the world of compliance management software, data security, and the rights of individuals with regard to privacy and control of their personal information.

However, GDPR and CCPA/CPRA were only the beginning of a cascade of data privacy regulations that dictate how companies around the world can (and cannot) use their customers' personal information. With clear mandates to return control of such data to customers—and stiff penalties for not doing so—organizations now have the arduous task of meeting compliance with an ever-growing set of regulations.

Data Privacy Management: Compliance is so essential (but hard)

Click on any icon to jump to a section.

In the beginning, there was GDPR. But now...

First there was the European Union's GDPR, then Brazil's LGPD, California's CCPA and CPRA, Canada's PIPEDA, India's DPB—the list can and will go on and on.

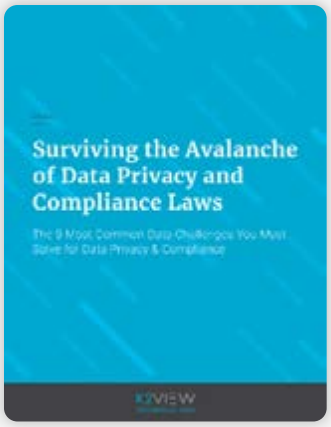
While each of these regulations originates in its own country, state or province, their reach is truly global: they affect every organization doing any kind of business with citizens in those jurisdictions. Each one, of course, is different in its scope and reach, not to mention the details of what compliance means and the potential penalties for non-compliance.

It's safe to say that no industry is immune or exempt from these mandates, given that every company has customers and therefore customer information stored on their systems.

The larger the enterprise, the larger the compliance target painted on its back. And the more siloed systems from which you have to unearth and correlate customer data to manage that risk and ensure compliance.

For these businesses, the ever-changing landscape of data privacy regulations likely means one of three things. Ignoring the mandates will lead to massive fines, and the brand damage and loss of customers could be of even greater magnitude. Handling the data subject access requests (DSARs) manually could cost almost as much—over $1,400 USD per DSAR according to Gartner. Or the organization can embark on a course of endless IT projects to handle each new regulation as it is passes—first GDPR compliance software, then CCPA compliance software, then—it doesn't end.

What other options does the enterprise have?



eBook: Surviving the Avalanche of Data Privacy and Compliance Laws

Businesses of all sizes scrambled to update their systems to meet the compliance deadline. But compliance isn't a systems problem. It's a data management problem. Discover how surviving the continuing wave of data privacy regulations requires a digital transformation in data management.

Download The Ebook

Common tenets of data privacy regulations

Whether it is GDPR, CCPA, LGPD, or any that have or will follow, there are some key data privacy concepts they all have in common. That is, they guarantee consumers a basic set of rights when it comes to their personal information:

- **The RIGHT to LAWFUL DATA PROCESSING** - You MUST have and divulge a specific, lawful purpose for storing and processing a customer's data.
- **The RIGHT to CONSENT (or NOT)** - You MUST allow consumers to agree to, refuse to, or withdraw consent to the lawful use of their data.
- **The RIGHT to ACCESS** - You MUST provide a consumer access to their data upon request and do so in a timely manner.
- **The RIGHT to BE FORGOTTEN** - You MUST comply with a consumer's request that you purge and completely erase their personal data.
- **The RIGHT to DATA PORTABILITY** - You MUST allow a consumer to "take their data and leave" and provide the data in an open, readable format.
- **The RIGHT to PRIVACY BY DEFAULT** - You MUST assume a consumer's data is private until consent is granted and ensure it is securely processed from end to end.
- **The RIGHT to NOTIFICATION** - You MUST alert consumers in a timely manner when their data has been affected by a security breach.

Overwhelmed by data privacy? Start with these 7 critical requirements

How alike or different are all these data privacy regulations? We'll show you.

View Infographic

At a minimum, companies have to ensure their data privacy management solution provides them the ability to protect these core rights for its customers—and flexible enough to handle the nuances that different regulations present.

Why businesses should care about compliance

n a nutshell, your organization should take compliance management seriously or it might not stay in business at all. If implementing a new compliance management software project each time a new regulation comes along sounds expensive, non-compliance can be financially disastrous to the enterprise. And it is getting more expensive with each passing year.

Manual compliance—that is, providing a form where customers can fill out a DSAR, then fulfilling it with manual processes—can actually be more expensive.

Some of the more involved DSARs include access to whatever data you have about them, to data portability, and to have their data purged. According to Gartner, the average cost of manually handling a single DSAR is $1,400—even higher for larger companies with customer information scattered across hundreds of applications and databases. Even if you anticipate a relatively low volume of customer requests, the costs can mount up quickly when your customer base is in the tens of millions.

As if the fines and operational costs aren't enough, there may be even worse consequences that affect the continued viability of the enterprise: broken trust with the customer and the inability to use their data going forward.

At a time when data is the new "oil," with every business striving to differentiate via customer experience—not to mention social media amplifying the voices of your company's advocates and detractors—this has vast implications that extend well beyond those created by fines or sanctions.

But compliance is often a long, difficult road

Smaller companies, whose customers number in the hundreds or in a limited geographical area and that have only a handful of operational systems and databases—can probably get by working DSARs manually on a one-off basis. In today's global economy, customers can be practically anywhere, subjecting the company to multiple data privacy regulations. Not to mention keeping track of the nuances and compliance requirements of every new regulation that comes along.

For larger enterprises, a manual approach simply won't scale.

The core of the problem, though, isn't the rapid appearance of new regulations. The problem for enterprises is that their customer data is managed by dozens or even hundreds of siloed systems and fragmented across as many data islands. This makes implementing compliance management software that maintains control over all that customer data—and satisfying all the requests for customer consent, portability, purging, and so on— a nightmare for large organizations.

Traditional approaches won't do

Traditional approaches to fragmented enterprise data have big drawbacks. And that's before you even consider applying the rules necessary to satisfying data privacy regulations. And still others ultimately require extensive customization.

1. **Periodically dump all your customer-centric data into data warehouses or data lakes.** There is nothing wrong with data warehouses for historical or analytical purposes, but using them for data privacy management purposes is problematic. These warehouses aren't systems-of-record, so if a customer requests their data be updated, masked or purged, you are still tasked with going back to each source system and making sure they're scrubbed.

2. **Integrate all your customer data, essentially building your own data privacy compliance software.** After all, every organization has its own unique mix of applications and databases, so why wouldn't compliance management require a custom software solution? But massive data integrations are cost-prohibitive and require constant maintenance. You'll constantly be signing up for costly new data privacy regulation comes along.

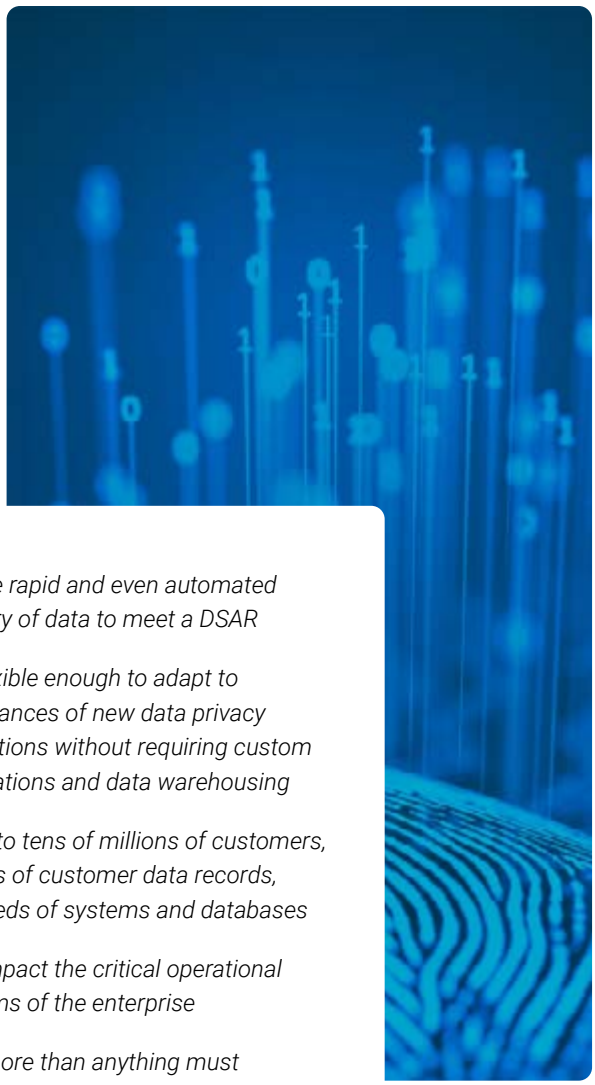
3. **Implement data privacy workflow management software.** Automating case management workflows, monitoring, and reporting for handling DSARs is only half the job! It still leaves the "heavy lifting" of the data to manual labor—data privacy workflow solutions don't provide automated access to the customer data across all underlying systems, nor delete or mask certain attributes on demand. This still has to be done manually. Some compliance management solutions provide a one-way (read-only) data integration but can't update the source systems. And still others ultimately require extensive customization.

Compliance management isn't a workflow problem. It's a data problem.

Regardless of the drawbacks to these different approaches to data privacy management, ignoring the avalanche of regulations isn't an option.

The third approach—implementing data privacy workflow management software—is most common today. It tries to address data privacy as a people-and-processes problem, but it fails to address the data part of the problem. In other words, these case or workflow management tools only deal with the "front end" of Data Privacy, leaving the "back end" activities—the hard part—to manual labor.

For over 40 years, enterprises have been building and buying software to solve specific problems—so we've ended up with hundreds of customer-centric solutions—CRM, customer support, billing, customer feedback, self-service portals, churn prediction, credit scoring, fraud prevention, and on, and on—each with its own customer data. That means to fulfill a DSAR, you have to touch all these back end data sources.



To truly manage the complexity of data privacy and compliance requires a single, up-to-date, and complete view of every customer—regardless of how many siloed applications and databases that data comes from. A compliance management software solution must:

- *Provide access to a 360-degree view of the customer in real time to both the operational support staff and the actual customer*
- *Implement identity resolution algorithms to correlate customer records across systems and interactions, while the systems might have different customer identifiers*
- *Enable the careful orchestration of data purging across underlying systems*
- *Allow a single point of customer consent no matter how many systems and databases are involved*
- *Fulfill the basic tenets and rights that data privacy regulations demand*
- *Enable rapid and even automated delivery of data to meet a DSAR*
- *Be flexible enough to adapt to the nuances of new data privacy regulations without requiring custom integrations and data warehousing*
- *Scale to tens of millions of customers, billions of customer data records, hundreds of systems and databases*
- *Not impact the critical operational systems of the enterprise*
- *And more than anything must maintain the security of every piece of customer information the enterprise possesses*

The opportunity: Solve the data problem first

No one will argue almost every enterprise around the globe will eventually be touched by at least one data privacy regulation.

For larger, global companies, it is inevitable. None of those companies will suggest that manual workflows and processes can scale to meet the compliance management challenge of even one regulation, much less the avalanche we are already seeing.

The problem is that the sheer number of customer systems and databases, not to mention the massive amount of customer data in those siloes - makes accessing, controlling, and updating customer data to comply with the regulations one of the toughest challenges companies will face.

However, we truly believe that compliance management software must solve the data problem underneath. Truly addressing the data problem is the opportunity and the key to a rapid, efficient, scalable, and (yes) end-to-end compliance management software.

We invite you to explore the issue—and its solution—on **K2VIEW.COM**.

K2View Data Privacy Management is the only platform that actually solves today's and tomorrow's data privacy compliance problem.

Right out of the box.