Five Practical Privacy Compliance Best Practices to Know

Posted on February 17, 2022 by Kon Leong in Best Practices

This is part of Solutions Review's Premium Content Series, a collection of contributed columns written by industry experts in maturing software categories. In this submission, ZL Technologies co-founder and CEO Kon Leong outlines five practical privacy compliance best practices to know when dealing with global data regulations.

Despite all the talk about privacy in recent years, the difficulties of implementing privacy at the enterprise level have yet to be fully grasped. Like building a high-rise, it is one thing to draw out the blueprints, but another thing altogether to put the infrastructure in place and build it. The first wave of privacy has been mostly on the front-end consulting, policies, and procedures for privacy. The second wave is now rolling in, where companies are faced with how to execute—including the plumbing, infrastructure, and care and feeding of the system.

The good news is the market is getting more serious about privacy. The bad news is that the market is getting more serious about privacy—but doesn't know how to go about it. Complying with privacy requirements, such as those stipulated by the European Union's **General Data Protection Regulation (GDPR)**, demands a complete change in direction from how companies have historically managed their

data. For decades, company data has been kept in silos— segregated by data source, geographic locations, and applications.

So too has information management been compartmentalized into function-based silos with separate governance strategies for legal discovery, compliance, supervision, records management, and now, privacy. However, the market is just waking up to the fact that privacy demands a convergence of all the above **governance functions** on an enterprise-wide scale. In short, privacy knows no silos.

That Holy Grail of **data management**, unfortunately, is not going to happen overnight. It will not be a sprint but a marathon of consolidating data management across the enterprise. Having set expectations, here are some practical approaches to begin the marathon:

Privacy Compliance Best Practices to Know

Start with High-Risk Areas

Formulate the overall road map but start implementation by focusing on the first steps. Just as no one can successfully boil the ocean at once, it is fruitless to attempt privacy in a single go. Take advantage of the natural learning curve and prioritize tasks that involve the lowest hanging fruit in the beginning.

For example, file shares have long been a corporate dumping ground, accumulating everything from financial information, customer mailing lists, HR documents, to vacation photos and other non-work-related materials. This treasure trove of sensitive data is a good starting point because a little effort towards scanning and cleaning it can go a long way in mitigating privacy concerns. Most companies have not cleaned up this data in years, if ever, so an initial scan for risk hot spots is likely to indicate several areas that require close attention.

Get Comfortable with (Defensible) Deletion

Companies have shied away from **deleting data** due to the risk of accidentally discarding something that needed to be kept—for example, documents required for records management, legal, or compliance purposes. However, new privacy regulations have made it clear that there are also consequences for keeping too much data. Personal data is to be disposed of when it is no longer needed for its original purpose, otherwise, companies face fines (and increased cybersecurity risks).

If you can't keep everything, and you can't delete everything, how does one decide what to discard and what to retain? This is where defensible deletion enters the picture: the act of enforcing a corporate policy for deleting data that is no longer needed. While seemingly simple, it involves a deep analysis of document content and interplay between each governance function, so that data is only deleted if approved by all the necessary policies. This interdepartmental communication brings us to our next point.

Establish a Cross-Business Committee

Gather the stakeholders and form a committee. Just as data is siloed, so too are departments. Implementing privacy requires taking input across the organization and synthesizing it into a holistic strategy. For that, you need the stakeholders at the round table, including IT, Legal, Compliance, Risk, Records Management, Privacy, and **Line-of-Business Data & Analytics**. You will be surprised how many lessons from these departments can be applied as best practices in privacy. For example, the concept of classification and defensible deletion can be taken directly from a records manager's handbook and extrapolated on an enterprise-wide scale.

Make it a Company Initiative; Get Top Management Buy-In Early

In the case of **data governance**, getting buy-in from upper management may be easier than anticipated given the large overlap between mitigating privacy risks and other top priorities, such as litigation support, business productivity, and performance. Notably, the form of holistic **data management** discussed here will go a long way towards enabling analytics on previously out-of-sight data, while ensuring governance and privacy are accounted for throughout the process. Keep these added benefits in mind when charting your roadmap and select the path that delivers these high-priority functions early.

The 11 Best SQL Books for 2022 Based on Real User Reviews

The 6 Best Cloud Data Lake Solutions to Consider in 2022

The 12 Best Graph Databases to Consider for 2022


The 8 Best Data Management Courses and Online Training for 2022

The Growing Demand to Prioritize Privacy

In addition to regulators levying hefty fines to non-compliant organizations, there is another driving force: in this new digital era, individuals are increasingly aware of their data footprints and have a vested interest in preventing their personal data from being exploited. This newfound awareness has resulted in a growing consumer trend to prioritize privacy with their wallets.

Personal data can hide in every nook and cranny of the enterprise, and the issue of privacy cuts across all intersections, demanding a new approach for companies if they want to stay in the good graces of customers, employees, and regulators. However, this rebuild provides an opportunity for organizations to realize a whole new vision for how data is managed—and reap the benefits. The next steps are up to you.

Author | Recent Posts

Follow Kon

Kon Leong

Co-Founder and CEO at ZL Technologies

Kon Leong is the CEO and Co-Founder of ZL Technologies, a provider of enterprise-class information governance and analytics solutions. In addition to speaking at industry events, he regularly contributes to a number of publications, such as Harvard Business Review, Fortune, and Business Insider, on topics ranging from information management and data privacy to analytics and business leadership.

Share this:

Twitter | LinkedIn | Facebook

Tagged Compliance GDPR Kon Leong ZL Technologies