SPONSORED BY acl

GDPR: How to establish a strong defensible position

By Phil Shomura

Mistakes inevitably will be made acclimatizing to the General Data Protection Regulation (GDPR). How could they not? The European Union's (EU) sweeping legislation is every bit as transformative to data management as Sarbanes-Oxley (SOX) was to finance and accounting. Meeting these entirely new data-privacy expectations is extra complicated because the law leaves many details open to interpretation, including the manner in which each organization contextualizes the monitoring and measurement of controls. Forward-thinking organizations, as part of their overall GDPR planning, are incorporating strategies to blunt the potentially severe punishments the EU has promised to start doling out worldwide.

Creating a defensible position — one in which organizations can quickly, easily, and definitively demonstrate to regulators they're making reasonable efforts to comply — is both prudent and wise as new gold standards take shape.

While such a strategy won't erase all fines, it will help organizations prove their GDPR procedures are grounded in sound data-protection and business principles. And it can bolster credibility with regulators even when compliance efforts fall short, as they inevitably will during the early growing pains of this sweeping initiative. Done right, a defensible position also

Essential Steps to Create a Defensible Position

1. Establish GDPR strategy, controls, and procedures.
2. Secure executive endorsements and engage cross-functional teams, including IT, legal, operations, and business lines.
3. Ensure the compliance team has a single lens view of the entire organization.
4. Leverage solutions that automate monitoring, workflow, and alerts.
5. Employ continuous monitoring as a reliable, real-time way to understand compliance posture.
6. Be prepared to readily and routinely transform data into meaningful reports for internal and external constituents.
7. Harmonize with other data-management obligations and opportunities.
8. Create continuous-improvement loop to regularly update the organization's compliance efforts and help develop industry gold standards.

strives to internally identify shortcomings and perpetuates a continuous improvement cycle.

For those grappling with how to create a defensible position, consider this: a simple technology-driven program that provides a holistic, real-time view of data operations; continually monitors data for exceptions; alerts employees when deadlines are approaching; warns employees when non-compliance occurs; and delivers comprehensive reports on demand. When embedded in an overall strategic GDPR program, a defensible position can help protect organizations from the pain GDPR is capable of inflicting.

The Cost of Non-Compliance

The consequences of GDPR non-compliance are real; EU regulators have been clear that they will levy heavy fines to violators serving EU consumers, even when the organizations are located beyond the EU's borders. The most egregious issues will cost violators up to 4 percent of annual global revenue or €20 million, whichever is greater. Other infractions such as failing to have records in order will carry a 2 percent fine.

Fines were already amping up under existing data privacy laws. A recent PwC study found that in the United Kingdom — which is incorporating GDPR into its laws — the number of fines for U.K. data privacy issues doubled in 2016 over the previous year. Enforcement notices rose by 155 percent and resulted in 35 fines totaling €3.25 million.

Here are three critical components of building a defensible position to help protect your organization:

1. Guessing vs. Knowing

An organization's proclivity for spot sampling will prove dangerous in the GDPR era, revealing how little is actually known about its data troves and whether the organization is properly handling all its data assets.

The common yet woefully inadequate qualitative procedures are being supplanted by modern tools that enable organizations to know precisely when and where exceptions and anomalies occur.

Real-time, continuous monitoring across all data sources provides an accurate picture of true compliance. Instead of guessing their compliance level based on random sampling, data managers actually know where problems exist, leading to the ability to quickly remedy both individual problems and systemic issues.

Real-time alerts and triggered workflows can automaticallywarn the right people at the right time when non-compliant behavior is detected or a GDPR deadline is approaching. Furthermore, these rigorous new testing methods enable compliance teams to deliver valuable, comprehensive information to regulators during audits and attestation requests.

2. Automate to Insulate

The ability to create a credible defensive position lies in technology. Advanced solutions enable Data Protection Officers (DPOs), Chief Compliance Officers (CCOs), and other stakeholders to industrialize their data operations and reliably and cost effectively manage resources to identify problems, make course corrections, maintain smooth operations, and intelligibly report and respond to internal and external constituents.

Automation is the foundation that enables data managers to accomplish these herculean tasks, and it will be instrumental in insulating them from potentially harsh penalties.

3. Crystal Ball

Dashboards providing a single lens view of an organization's entire data population enable DPOs and CCOs to successfully guide their organization through GDPR-driven change in conjunction with other compliance mandates. They provide oversight across the entire organization, including any extended compliance measures required of third-party vendors.

Modern dashboards are the equivalent of a crystal ball: They provide a real-time, holistic view that illuminates trends and issues, all the way down to the individual level. A single lens view can efficiently identify where organizations are in compliance and, equally important, where they're not.

Superior Features that Set Apart Modern Solutions

- A single lens view across the organization's key control measures to assess compliance posture
- Automation to free staff time for strategic endeavors and critical remediation
- Continuous monitoring to replace outdated, unreliable spot-check testing
- On-demand reporting for attestation of controls and proof of effective compliance measures

At any time, data managers can assess risks with an aggregate view of existing controls to manage and demonstrate compliance efforts.

The quantitative data derived from an organization's entire data population removes uncertainty and helps establish a defensible position.

The automated oversight combined with data analytics and automated workflow frees organizations from manual compliance validation to focus on the strategic big picture. The insights, of course, feed back into the crystal ball.

Benefits Beyond GDPR

Modern governance software systems allow data managers to split regulatory obligations into requirements; map controls to these requirements to assess applicability and coverage; and determine compliance gaps. What's more, they can also help harmonize other data privacy principles from established frameworks (ISACA, NIST, ISO, COBIT) with a many-to-one mapping to single controls. Confidence that controls are effective is fueled by insight into the entire data population.

Conclusion

GDPR is dictating extraordinary change in data-protection practices. As organizations strive to create modern gold standards, lessons will be learned. The best opportunity to avoid harsh penalties and participate in influencing the gold standards is for organizations to create a defensible position.

Technology will help organizations work smarter while developing a quick-to-serve defensible framework. Intelligent, automated workflow solutions will remove the uncertainty and replace complexity in GDPR compliance.

For More Information

To learn how ACL can serve as a resource to help create a defensible position for GDPR compliance, visit acl.com.

Phil Shomura is a senior product manager for ACL, a provider of enterprise governance software driven by data automation.