Grant Thornton

The EU raises the bar on data privacy:

AIM for an integrated response

Organizations can view the EU's General Data Protection Regulation (GDPR) as either a problem or an opportunity. Grant Thornton sees opportunities to enhance performance and competitive position, as well as ways to reduce compliance costs, complexities and problems.

The EU's GDPR goes into effect on May 25, 2018, with potentially far-reaching effects. Yet, many affected companies will be unprepared. Gartner, Inc. "predicts that by the end of 2018, more than 50% of companies affected by the GDPR will not be in full compliance with its requirements [1]." Lack of preparation for new compliance typically stems from uncertainty about what to do, which is understandable. The rigor of enforcement, unpredictable regulatory priorities, and needed process and system changes can all be difficult to determine.

Yet, organizations must take priority in responding to this regulatory mandate. The GDPR, which will affect EU data controllers and processors, as well as many outside the EU, goes well beyond the 1995 EU Data Protection Directive. The GDPR calls for fines of up to €20 million or 4% of annual revenue, whichever is greater — the latter being a major hit to the net margin for most companies. Like most regulatory initiatives, the GDPR raises the prospect of public censure and reputational risk. GDPR privacy rules are stringent, and organizations must demonstrate compliance to avoid regulatory action.

EU's GDPR goes into effect on May 25, 2018

More than 50%

of companies affected by the GDPR will not be in full compliance with its requirements.

20 million or 4%

of annual revenue in fees, whichever is greater — the latter being a major hit to the net margin for most companies.

[1] Gartner, Inc. *"Gartner Says Organizations Are Unprepared for the 2018 European Data Protection Regulation"* (press release), May 3, 2017.

How an organization responds to the new regulations will either increase or reduce governance, risk management and compliance (GRC) costs and complexities.

Grant Thornton sees GDPR not only as a compliance challenge, but also as presenting opportunities for companies to enhance performance-driven risk management [2]. At its heart, this regulation aims to enhance the ability of individuals to exercise rights over their personal information, thus addressing widespread consumer and government concern regarding personal data and information security.

Organizations that can demonstrate to customers, employees, suppliers and other stakeholders that they can properly secure their personal data and information may well gain advantages over those that cannot. In addition, designing and operating organizational processes and systems in ways that enhance both the protection of personal data and the ability to respond to data-related requests can — when approached in an integrated, risk-based manner — drive performance improvements.

Whether an organization's senior executives and board see the GDPR as presenting opportunities or problems, this much is certain: How an organization responds to the new regulations will either increase or reduce governance, risk management and compliance (GRC) costs and complexities. That has been the experience of most organizations with regard to virtually all major regulatory initiatives, with the Sarbanes-Oxley Act of 2002 (SOX) as a good example.

2. Grant Thornton. Performance-driven risk management: An integrated approach, April 2017.

Look backward to see forward

SOX set new and expanded requirements for all U.S. public companies and public accounting firms, and created requirements for privately held companies. In response, organizations scrambled to improve their internal controls, corporate governance and disclosure, and reporting mechanisms.

Indeed, SOX revealed a pattern that many companies tend to follow in response to major regulatory initiatives — a pattern reflected in many companies' current GDPR efforts.

Among the most common characteristics of this pattern are:

Efforts to achieve blanket compliance

GDPR features 99 articles, but how these requirements will apply to a given organization will depend on its operations, customer base, risk appetite and desired risk profile. We cannot know how vigorously requirements will be enforced until the first year or two after GDPR takes effect. Thus, a risk-based approach to considering and implementing GDPR compliance will be preferable to blanket approaches.

Complicated processes and programs

Crafting specific responses to each individual mandate adds to the complexity of compliance. For example, the GDPR's required data protection impact assessment (DPIA) may prompt a company to put all new products, technologies and services using personal data through a DPIA. Yet, companies are already conducting security, business continuity and other data-related assessments. Each added assessment adds costs and, potentially, another data-gathering and reporting silo. Leveraging existing assessments can reduce costs, as well as complexities.

Overspending on tools

Companies facing new regulatory mandates often buy compliance-focused tools in hopes of obtaining efficiencies, and privacy tools have moved into this already crowded marketplace. Many new privacy tools resemble traditional GRC tools in that they feature requirements repositories, user surveys, email-driven workflows and reporting capabilities. Before buying any GDPR tools, the organization should review current GRC tools with an eye toward reducing costs and integration challenges.

Separate compliance and risk-related responsibilities

Companies facing new mandates often appoint someone to oversee compliance. With the GDPR, this person may be in the compliance, legal or privacy area. However, responsibility for managing the related risks should reside with the appropriate managers in the businesses and functions where those risks can be controlled. This can be tricky because responsibilities for complying with the regulation may be assigned to a party other than the one responsible for the risks. When that is the case, the two parties must communicate effectively to resolve competing priorities, which takes time and skill.

Further fragmentation of GRC

The foregoing factors can undermine GRC integration in the organization by creating new silos and reporting streams, and obscuring accountability. Reacting to the GDPR can create overlaps, redundancies and gaps that hinder compliance while creating another isolated compliance program and, potentially, new risks.

Failure to sustain the program

Companies often work hard to comply with new regulatory mandates, but fail to build in sustainable processes and systems. Those facing the need to comply with the GDPR must bear in mind the need to sustain compliance beyond the May 2018 deadline. This calls for training business users in privacy matters, centralizing customer preferences and consent management, designing solutions with privacy and security in mind, and leveraging existing compliance efforts and technologies.

These issues tend to emerge around any major regulatory initiative, and addressing them calls for understanding how the organization may be affected and potential costs and complexities. With that understanding, management can develop a thoughtful response.

Don't react — respond

Most major regulatory initiatives elicit similar reactions. Companies' compliance efforts usually peak in the year before the effective date, and remain strong in year one and into year two. Absent vigorous enforcement, efforts tend to ease because compliance is a cost to be minimized when possible. This approach can create costs and risks of its own. For example, more vigorous enforcement may occur under a new political regime or after a high-profile breach. Companies caught off guard find themselves incurring extraordinary costs to mount a suitable response. If a breach occurs at your company, the financial, strategic, and reputational risks and repercussions can be substantial.

Thus, your company's goal should be to increase the certainty around multiyear planning for GDPR. Your company should focus on maximizing the integration of GDPR compliance with the GRC program, with the goal of minimizing the data-related risks rather than achieving total compliance. This leaves your organization reasonably well-prepared while controlling costs.

5 Steps to minimize data-related risks

1. **Learn what applies**
   The key GDPR mandates for your organization will include those enabling your customers to request actions or information related to their personal data, those related to customer or employee complaints, and those involving data breach notifications and vendor management requirements. If you establish sound practices in these areas and set up key risk indicators to monitor the GDPR program, you can keep the compliance effort to a reasonable size.

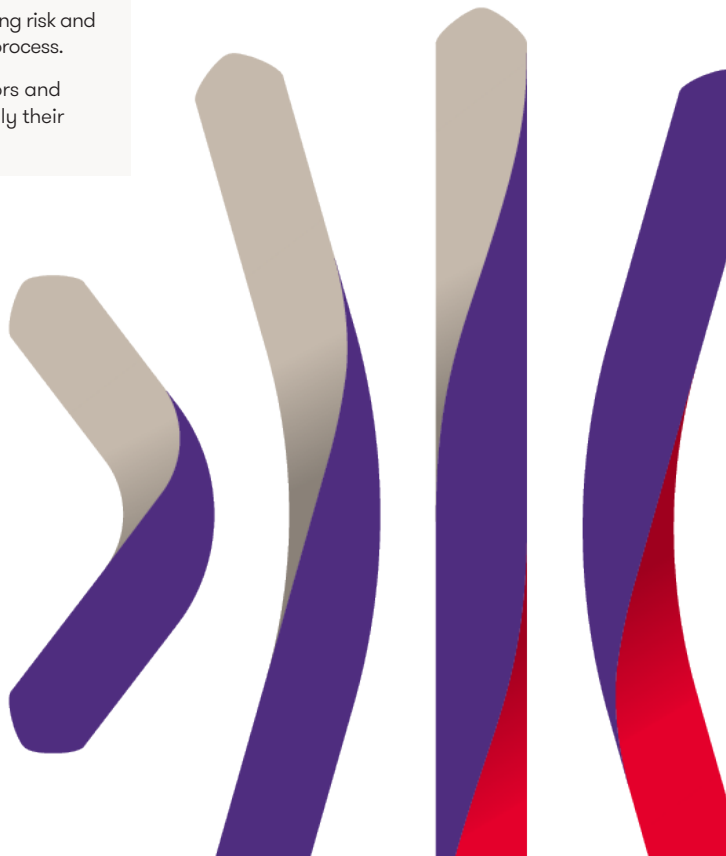
2. **Take a risk-based approach**
   In practice, every compliance decision is a risk management decision. While compliance with GDPR is mandated, each company faces decisions: How will we decide where to invest and in what resources or efforts? Which areas present the greatest compliance, financial and reputational risks? In what types of resources and efforts will we invest? Answering those questions enables you to allocate investment to the highest-risk areas or those posing risks beyond a certain threshold. A risk-based approach identifies high-risk activities and systems related to personal data collection, processing and sharing, and then developing appropriate steps based on the risks and costs.

3. **Evaluate what you have**
   Before creating another process or more checkpoints, evaluate what you can leverage from existing assessments, reviews and audits. This may enable you to gather needed data without creating another process, burdens and costs, or perhaps to integrate a privacy requirement into existing assessments. For example, in vendor due diligence, combining DPIA with a security assessment that uses one security, privacy and compliance questionnaire could reduce both the cost of compliance and redundant assessment activities.

4. **Consider new tools carefully**
   Many organizations have spent huge sums developing GRC tools to support SOX, internal audit, data security and controls testing. When you look under the hood, the features and workings of these tools are quite similar. So before investing more in software and licenses for privacy, review your systems and assess the extent to which you can use them to fulfill GDPR requirements.

5. **Work within your GRC infrastructure**
   To prevent more siloed compliance efforts, management must ensure that risk management, legal, compliance, privacy and security functions coordinate with each other. The GDPR program should be integrated into an overall governance infrastructure for managing risk and compliance, following a coordinated executive and board oversight and reporting process.

Organizations affected by GDPR owe it to themselves and their customers, investors and other stakeholders to view GDPR compliance as an opportunity to enhance not only their processes and systems but related risk management capabilities as well.



Toward a performance-driven approach

When not integrated into existing GRC efforts, responses to major regulatory initiatives tend to increase GRC fragmentation, costs and complexities. Adding new activities and reports may be inevitable; however, to the extent that the existing GRC infrastructure can be leveraged, the downsides can be controlled. To the extent that new needs cannot be met with current capabilities, new capabilities should be carefully considered and integrated with existing processes and systems.

In fact, given stakeholders' often justified concerns for the security and privacy of their data, integrating certain GDPR-mandated features into processes and systems simply makes sense. For example, GDPR Article 17 "Right to erasure ('right to be forgotten')" and Article 25 "Data protection by design and by default" each require capabilities that may or may not exist in current systems. However, designing future processes and systems with such erasure, protective and consent management capabilities might make sense from a competitive standpoint, even for organizations not subject to the GDPR.

Extended enterprises should ascertain the extent to which affiliates, partners and other third parties present compliance, privacy and other data-related risks as a result of the GDPR. Again, the GDPR may present opportunities to enhance controls on such risks and integrate them into the third-party screening, selection, onboarding and management process. The more efficiently and effectively an organization can do this, the more competitive it will be.

Sustaining GDPR compliance calls for automating data privacy and security to the greatest possible extent. It takes time to clarify roles, rationalize controls, and squeeze waste out of processes and systems — all prerequisites for moving from manual to automated processes. But the sooner you begin, the better. Look for ways to adapt currently automated risk-related processes to GDPR purposes. Also, establish collaboration between legal, compliance, privacy, risk management, IT and security functions to promote the cooperation needed to facilitate automation.

Consider the ways in which you digitally interface and plan to interface with customers, prospects and other stakeholders.

1. How might your cyberstrategy be affected by the GDPR and its considerations?
2. Which data do you collect or intend to collect, and how does that dovetail with the goals of the GDPR?
3. How might the issues raised by the GDPR affect your current and planned strategies for using social media or monetizing customer data?

Asking and answering these questions elevates GDPR compliance from a tactical, regulatory issue to the strategic issue that it actually is for companies that collect, store, process and use customer data.

The keys to successful GDPR compliance are:

- Take a risk-based approach to understanding how GDPR applies to your organization.
- Leverage existing compliance efforts to prepare for GDPR and enhance overall risk management.
- Clarify ownership and responsibility for compliance and risk management, and establish a strong coordination function.
- Control costs from the start of the initiative instead of throwing money at the effort.

For more information on ways in which Grant Thornton can help your organization address compliance and risk management needs, visit **gt.com/risk.**

To learn more about our approach to align, integrate and measure (AIM) cyber risk outcomes, download our white paper, ***Taking AIM at cyber risk.***

Contact

Vishal Chawla
National Managing Principal, Risk Advisory Services
T +1 703 847 7580
E vishal.chawla@us.gt.com

Derek Han
Principal, Cyber Risk
T +1 312 602 8940
E derek.han@us.gt.com

GT.COM