Tackling the Complexity & Uncertainty of Compliance in Privacy and Data Protection

Insights and Success Tips from Veteran Privacy and Information Security Officers

WISEGATE COMMUNITY VIEWPOINTS

wisegate

300 Beardsley Lane | Suite C201 | Austin, Texas 78746 | www.wisegateit.com

Introduction

As the public has become more aware of privacy issues and the need to protect private information from public disclosure, governments and industries have acted to expand the legislative and regulatory requirements that companies must meet. Today's senior privacy and security professionals face a complex web of regulations, cross-border data privacy requirements and evolving compliance risks, like the use of social networks in the workplace.

The members of Wisegate work for multinational corporations, educational institutions, governments, and non-profits in virtually every industry – retail, banking and finance, energy, medical and healthcare, insurance, education, government, and more – and have responsibility for the successful oversight of major corporate and enterprise-level IT compliance and risk management programs.

Even at their level, these top executives want access to a senior group of peers who can help each other successfully address the complex legal, regulatory and security issues they face. That is one reason they join Wisegate—to have others in a virtual peer group who have no financial interest in a decision and who can share their experiences and advice. They trade war stories, compare how to approach a problem, and share best practices.

In this report, you'll get an inside view to the practical advice and insights that Wisegate members usually only share privately with each other through the Wisegate Privacy and Compliance micro-community. These tips provide insights into how senior privacy and security officers from Fortune 1000 companies are balancing an increasing number of privacy and data protection rules with the need for continued business growth and innovation.

Monitoring the Regulatory Environment

There are numerous U.S. state laws and a number of U.S. federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), which contain privacy and data protection requirements. And there are international laws, such as the EU Data Privacy Directive, that companies doing business in Europe have to comply with.

Wading through all those laws and regulations can cause even the most seasoned IT privacy/compliance professionals to throw up their hands in despair. Wisegate members successfully deal with this legal and regulatory morass on a daily basis and offer the following advice for monitoring the regulatory environment.

- Keep track of regulatory changes through listservs and email bulletins that provide updates on regulation. Sign up for bulletins distributed by federal agencies that cover your industry. For example, the Federal Reserve provides automated notifications on privacy issues affecting the financial industry.
- Sign up for a compliance monitoring and information service, such as Nymity, Unified Compliance Framework (UCF), Archer, Paisley, International Association of Privacy Professionals (IAPP) alerts, etc.
- Share information among people in your company who follow privacy and data protection regulation. *"Monitoring is a joint effort between the compliance department, legal department, privacy officer, and information security officer. We work very closely together to keep up and keep everyone informed."*
- Set up an alert notification system within the company that alerts those who need to know that a regulatory change is coming.
- Establish a cross-functional executive team that includes those who follow privacy and data protection in the company, as well as C-level executives. Have the committee go through the new regulations and decide which ones are required and which ones are advisable for the company to implement. *"We have a cross-functional executive team that I chair that has legal audit, risk, and governance, and has the chief financial officer on it, and we go through all the regulations and all the new things that come through and decide what is necessary for the best interest of our organization."*

Analyzing Legislative Changes/Legal Precedent

While keeping up to date with regulations is challenging, understanding how legislative changes and legal precedent impact your bottom line is downright maddening. Of course, if you have a legal department, they can help you with that. But the lawyers often abstain when the conversation turns to translating legal changes into privacy and data protection policies and procedures. Wisegate members offer some tips of the trade.

- Review new legislation and court decisions to see where the impacts are for your organization. If policies need to be changed, rewrite the policy and send updates to the affected areas in the business. *"I'll review legislation along with the privacy officer. We'll determine where the impacts are and make whatever adjustments that we have to do in order to make it effective in our organization."*
- Prioritize legislative changes and legal precedent according to how they affect your business. For example, a non-health multinational operating primarily in Europe

should track EU privacy and data protection directives closely, but not worry so much about HIPAA changes in the United States. Conversely, a healthcare organization operating primarily in United States should track HIPAA very closely.

- Set up regional privacy and data protections groups that follow legislation and court decisions in that region.
- Add legislation changes and legal precedent to a risk register and then prioritize them along with other risks. *"We add [legislative or legal changes] to our risk register and then prioritize this like any other risk to the company. Once all of the risks are prioritized we treat, tolerate, terminate, or transfer each risk."*

Integrating Emerging Requirements

What is the best way to ensure that emerging requirements are integrated into privacy and data protection policies and procedures? Using privacy impact assessments and risk mitigation plans and mapping new requirements to an existing standard, such as ISO 27001/2, are a number of the suggestions offered by Wisegate members.

- Perform privacy impact assessments on personal data processing. The assessment should trigger certain inquiries. If the question is asked: Does this data processing include health data, then you know you have to look at HIPAA and Health Information Technology for Economic and Clinical Health (HITECH). *"We perform what we call privacy impact assessment on any instances of personal data processing…We address emerging requirements in that way."*
- Develop and implement a risk mitigation plan that includes privacy and data protection, and allow the business units to determine the risks they are willing to take regarding protecting personal data. This pushes responsibility out to the right people in the organizations rather than trying to have the privacy officer be responsible for everything in the organization.
- Distribute questionnaires to business units about what information might fall under privacy and data protection requirements, as well as steps the units are taking to mitigate the risks to that information. *"We have a questionnaire that we ask the businesses to fill out. We then do a formal executive summary of the processing activities which include a risk evaluation and a risk mitigation plan or suggested risk mitigation plan."*
- Rank business units according to privacy and data protection performance. This creates competition and peer pressure to do a better job.

- Map emerging requirements to a base standard, such as ISO 27001/2, and use a governance, risk, and compliance (GRC) tool. This makes it easier to integrate emerging requirements as well as explaining what certain changes need to be made to employees. *"My philosophy is based on comply-once, comply-to-many and built around COBIT, ISO 27001/2, and ITIL focused first on the 'must do' regulated environment…Then use an UCF or a GRC tool (Archer, Paisley, Lockpath, etc.) to cross-map regulatory needs to help apply, govern, and document controls for an industry regulation such as PCI DSS (or SOX 404, HIPAA, etc.) and then simply hit the button to find out where your gaps are for other regulations."*

Overcoming Objections

It is all well and good to use personal connections and compliance tools to monitor regulatory, legislative, and legal changes, and then move to implement them. But what happens if you get "push back" from people within your organization? What if your U.S. personnel do not understand why they need to comply with the EU Data Privacy Directive? Wisegate members recommend educating your employees about the need to make changes. But, in the end, if changes have to be made, as one member said: *"We don't entertain objections."*

- Do not consider objections to regulations and legislation that must be implemented for your industry. *"We don't entertain objections. The regulations say we have to do it, so it's something we have to do."*
- Educate employees about the risks and requirements through the privacy impact assessment and through a corporate data policy. *"We use a part of that [compliance] process as an education of people as to why this needs to be done."*
- Have a point-person in each department who can handle objections and complaints and explain the reasons for the changes to policy and procedures.
- Recognize regional differences in terms of objections and develop a consultation process to deal with those differences. For example, the EU Privacy Directive is very strict, and the U.S. staff might not understand the need to adopt EU rules.
- Work with legal and the business side to guide the organization towards safe practices. *"At the end of the day, regulations are there to keep us all accountable to provide a standard of care and ensure that there are some guidelines to avoid negligence."*

In Closing…

We hope that these tips from Wisegate members help make your job easier and give you the insights you need to successfully navigate the evolving complexity of legal, statutory, and regulatory privacy and data protection issues. As regulatory bodies continue to bombard privacy and security professionals with new challenges and job-related headaches, the conversation on how to quickly and decisively address even the most perplexing compliance issues continues on wisegateit.com.

Wisegate is the invitation-only community where senior IT professionals meet to exchange knowledge and solve problems with their peers. It is Wisegate's mission to make our members' job less stressful and more productive by providing the social knowledge network professionals need to collaborate and share experiences with a closed community of highly qualified IT peers. By enforcing strict membership guidelines, which exclude vendors from joining, Wisegate is able to provide members with unmatched access to senior-level IT professionals and quality content.

Would you like to join us? Go to wisegateIT.com/request-invite/ to learn more and find out if you qualify for membership.

wisegate

300 Beardsley Lane, Suite C201

Austin, Texas 78746

PHONE 512.329.6444

EMAIL info@wisegateit.com

www.wisegateit.com