Special ISA NewsFlash! 5/3/2018
European's General Data Protection Regulation (GDPR) - Are You Ready?

Bold Thinking. Smart Growth.

Hello ISAers,

I am sending this special notice and information for two reasons:

1. **To call attention to** the looming deadline and potential implications of the European's **General Data Protection Regulation (GDPR)**. The attached article, while written for association executives, is a useful summary of what GDPR is all about.
2. To inquire as to interest or need among ISA firms. ***If you are interested in coming together*** for a conference call or webinar to compare notes and/or learn more, ***please let me know***. Your prompt response via the form link by May 17th will be helpful.

Recent conversations with members of ISA have called attention to the regulations specified in the European Union's General Data Protection Regulation. Many of you are already aware of the looming May 25th deadline but some of you are unaware of the deadline or what this may mean to your business. The regulations are a fundamental shift in how personal consumer information must be processed and secured across 31 countries known as the European Economic Area (EEA.) The 99 articles adopted in May 2016 will apply not only to EU businesses, but also to any company or organization with personal information about individuals located in any of the 31 countries (EEA countries).

While this has been in motion since 2016, the recent Facebook hearings and data privacy issues that are in the news has heightened concern related to "data access and accessibility." It's important to pay attention to how these discussions and challenges impact business practices in the short and long term. For example, failure to comply with the regulations can be costly - up to 4% of a company's annual global revenue or €20 million.

Thank you!
Pam

Pamela J. Schmidt
ISA Executive Director

P.S. - Additional information about GDPR:
For a copy of the PDF for European Union data protection regulation:
https://thinkgdpr.org/article/regulation-eu-2016679/

Privacy Shield Framework - https://www.privacyshield.gov/welcome
Privacy Shield Program Overview - The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

CSO serves enterprise security decision-makers and users with the critical information they need to stay ahead of evolving threats and defend against criminal cyberattacks. With incisive content that addresses all security disciplines from risk management to network defense to fraud and data loss prevention, CSO offers unparalleled depth and insight to support key decisions and investments for IT security professionals. CSO Article: GDPR Requirements and Facts

associations now MAR/APR 2018

COUNTDOWN TO GDPR: WHAT ASSOCIATIONS SHOULD KNOW

May 25 is the looming deadline for organizations to comply with the European Union's General Data Protection Regulation, and many are not prepared for this fundamental shift in how personal consumer information must be processed and secured. Ready or not, enforcement is coming. Here's what you need to know as May approaches, especially if you're behind the curve.

On the desktop of Carol Tullo's computer screen sits an ominous countdown clock. It ticks down the days, hours, minutes, and seconds to May 25—the date when the European Union's long-awaited General Data Protection Regulation takes full effect and when enforcement, with its threat of costly penalties, kicks in.

Tullo, an associate consultant with the UK-based consulting firm the Trust Bridge, has been coaching businesses and organizations on the compliance implications of GDPR. Adopted by the European Commission in May 2016, the regulation encompasses a set of rules that harmonizes data and privacy protection laws for individuals across 31 countries—all 28 EU member states plus Iceland, Liechtenstein, and Norway, known collectively as the European Economic Area (EEA).

The May 25 enforcement date marks a pivotal moment. Despite a two-year grace period for organizations to implement GDPR-compliant internal data practices and policies, Tullo says, many associations have not taken adequate steps to prepare. In an August 2017 survey by the IT governance association ISACA, fewer than one-third of senior executives and boards of directors (32 percent) said they were satisfied with their organization's progress to prepare for GDPR. More than a third (35 percent) said they were unsure of their progress.

While it may be tempting to shrug off GDPR because your members or customers are not primarily based in the EU, the broader implications affect businesses and organizations globally.

"This is a wake-up call for all organizations," Tullo says. "GDPR doesn't stop on May 25, when it comes into full effect. This is about building long-lasting and conscious trust with your customer and making sure you have the data hygiene and confidence in place for a new way of doing business."

Broad New Protections

GDPR significantly enhances the rights of data subjects in the processing of their personal information. Under the new regulations, EU residents have the right to access their personal data, the right to rectify incomplete or inaccurate data, the right to be forgotten, and the right to restrict the processing of their data.

Organizations will have about 30 days to respond to individual requests about whether personal data is being processed and, if so, to provide access to that data. And if an organization experiences a data breach, it will have 72 hours to notify EU data protection agencies. Failure to do so could cost you: Violators are subject to fines up to €20 million or 4 percent of a company's annual global revenue, whichever is greater.

GDPR's 99 articles apply not only to EU businesses, but also to any company or organization with personal information about individuals located in the EEA countries.

A key concern for many organizations is how broadly personal data is defined. The European Commission says it's "any information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a photo, an email address, bank details, your posts on social networking websites, your medical information, or your computer's IP address."

The regulations also prohibit the processing, without consent, of sensitive data on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sex life or sexual orientation.

Team Effort

To reach compliance, association staff at all levels—from the CEO and senior executive team to marketing managers and membership coordinators—need to understand their role in proper data management.

"People make the mistake that data security is only about the technology, but it's not," says Keith Moulsdale, a partner at the law firm Whiteford Taylor Preston, LLP. "It's about administrative, physical, and technological compliance, which is a team effort."

Accept and embrace the fact that privacy compliance will be an ongoing fact of life well beyond this date. The reality is that most associations probably won't reach full compliance by May 25, and that's OK, says Razvan Miutescu, counsel at Whiteford Taylor Preston and the firm's lead on GDPR. But they'll need to get up to speed as soon as possible.

"Accept and embrace the fact that privacy compliance will be an ongoing fact of life well beyond this date," Miutescu says. "Taking a reality check and engaging in active prioritization is key. Identify the biggest risk exposures specific to your organization and start the compliance process there—one at a time and without letting the concerns of the broader noncompliance status paralyze that effort."

At the Institute of Food Technologists, the point person for risk assessment is Tom Foley, vice president of membership and customer development. His day-to-day job is overseeing data integrity for the organization, and he is currently at the helm of IFT's GDPR response plan.

"In some ways, the starting point is doing an in-house gap analysis," he says. "Identify where you are weakest, and how your overall data strategy should change."

About 15 percent of IFT members reside outside of the United States in more than 90 different countries. In addition to GDPR compliance, Foley has been focused on other global regulations like Canada's Anti-Spam Law and China's Foreign NGO Law.

"We're trying to take a holistic approach here so that we're not just reacting to the EU and GDPR, so much as what else might be on the horizon," he says. "A big part of our data management strategy is being transparent and asking: Do we really need that data?"

Road to Compliance

Associations typically have data records that stretch across multiple software systems and through a variety of data-processing streams.

"Too often data is kept all over the place," Tullo says. "So, first and foremost, you have to know what you've got and where you've got it. This is a timely moment to revisit and refresh your data practices."

In advance of May 25, many organizations are either deleting data or conducting data "pseudonymization"—a process that separates data from direct identifiers, so that it can't be linked to personal information without additional information that is held separately.

Many association data systems are maintained by third-party vendors, who are themselves gearing up for GDPR and may be able to serve as advisors in your compliance effort. At the very least, says Larry Samuelson, senior vice president at Cvent—a provider of event management software—you should be talking to your vendors and revisiting each of your vendor agreements.

To reach GDPR compliance, Cvent spent nine months establishing new vendor agreements bound by the Privacy Shield, an approved framework for privacy protections for EU-U.S. exchanges of personal data.

"We worked with all our vendors and sub-processors to make sure they were handling information the way we told them," Samuelson says. "And some vendors couldn't do it, so we discontinued or fired them."

Internally, Cvent undertook a data-mapping exercise, a specific requirement of GDPR compliance. Critical to this exercise are five key questions:

1. What data does the organization handle?
2. Where does it come from?
3. How is it being processed?
4. Why is it being collected?
5. Is it necessary for business operations?

“As the controller [of the data], you’re responsible for answering these questions,” says Pradeep Mannakkara, chief information officer at Cvent. “Data mapping is one of the most critical things that every association should consider . . . and hopefully you’re also asking: Are my vendors compliant?”

The three words in GDPR that Samuelson says are key to determining what data can be collected are “legitimate business interest.” If you have a legitimate business interest in a type of data, you can make the case for processing it. But take care how you gather even seemingly innocuous information, lest you inadvertently steer into noncompliance.

“Imagine if you ask somebody if they’re kosher or halal” on an event registration form, he says. “Well, that goes to religion. What you could say instead is: ‘Are you vegetarian?’ or ‘Do you eat meat?’ I do think you have to re-engineer those levels of questions to understand what your legitimate business interest is.”

Organizations are also rewriting their privacy notices to clarify how personal data is collected, processed, and stored.

“Your privacy notice is a public message about what you plan to do with personal data,” Tullo says. “Keep that statement simple and in plain English. It’s almost like saying who you are as an organization.”

Tipping Point

GDPR is a fundamental shift in how data is processed and secured, and Moulsdale thinks the right of individuals to control their data will only grow as other countries adopt similar regulations.

“We’ve reached a tipping point because the momentum has built behind the EU’s approach to privacy in a way that’s tipping other countries to change their laws, and in doing so, changing business practices,” he says.

Tullo agrees that GDPR signals the beginning of a long-term evolution in data management. “Really, this is about changing people’s approach to data,” she says. “Come May the 25th at midnight, we certainly won’t fall off a cliff. Instead, think of this as a starting point—a continuous push for trust, confidence, and transparency to run your business.”