COMPLIANCE WEEK
THE LEADING RESOURCE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

GDPR compliance is lagging

A survey says many firms are nowhere near ready to comply with the new EU data privacy standard. **Jaclyn Jaeger** has more.

With just months to spare before the EU's General Data Protection Regulation takes effect, many firms say their data governance practices still are not up to snuff.

That finding emanates from a survey conducted by Compliance Week and data governance platform provider Collibra to assess companies' readiness with the GDPR, which will take effect in May 2018. The GDPR will replace the EU Data Protection Directive enacted in 1995 and will create a uniform approach to data protection laws across the European Union.

"The GDPR is not just about data protection, as its name suggests," Tudor Borlea, sales engineer and GDPR specialist at Collibra, said during a Compliance Week Webcast discussing the survey results. "It's about protecting the rights of data subjects."

"It's about driving culture, using personal data responsibly and transparently," Borlea said. Specifically, being GDPR compliant means being responsible and transparent about how personal data is used, who owns it, who has access to it, how it moves across borders, and then being able to document all of that.

One of the key changes is the global scope of the GDPR's application. The GDPR applies to any company—even those outside the European Union—that offer goods or services to EU residents or that processes personal data within the European Union. It also broadly applies to both data controllers (those who collect and own the data) and data processors (essentially, third-party vendors). Any organization that is unsure as to what category it falls under may want to seek guidance from its lead supervisory authority.

Penalties for non-compliance are now more severe than ever. Companies that don't meet the new requirements can face fines up to 4 percent of total annual global revenue or €20 million ($21.5 million), whichever is higher.

The findings of the Collibra survey reveal, however, that some companies do see the business value in GDPR compliance. Of 111 executives polled, 41 percent said they agree that GDPR is "a way for the organization to showcase its privacy program." Thirty-one percent said they are not sure, while 27 percent disagreed with that statement.

The demographics of the survey respondents covered a broad range of both large and small companies from around the world—North America, Europe, and elsewhere. Companies ranged in size from less than 250 employees to more than 100,000 employees.

The results further revealed that many still don't feel fully prepared to be considered GDPR compliant, with 61 percent saying they are "somewhat prepared," indicating that they're in the process of tweaking their data governance program and are on track to make the deadline. Just three percent said they're "very prepared," believing their privacy principles are robust and that no changes will be required.

And 22 percent said they're "not at all prepared," that they've just begun to adopt privacy principles for the first time. Although becoming GDPR-compliant likely will be a daunting task for these respondents, Borlea said, it certainly won't be as daunting as for the 14 percent of respondents who indicated that they haven't even thought about GDPR yet.

Survey respondents were also asked whether they believed GDPR will require a cultural shift, a question that garnered a 50/50 split among respondents. "In my opinion, GDPR does require a culture shift," Borlea said. "That is the key to unlocking GDPR compliance, being able to permeate an entire organization with this new way of thinking about data."

When asked what governance approach they are taking, the plurality (37 percent) said they are taking a dual "top down" and "bottom-up" approach. This means they are "starting with the principles, standards, stewardship, and data-processing activities," as well as "starting with the data discovery." If time and budget resources allow, a dual top-down, bottom-up approach is recommended, Borlea said.

The second biggest group of respondents (26 percent) said they are taking neither approach and that they haven't started yet. This finding correlates with the overall lack of preparedness many respondents answered in the previous question.

Another 22 percent said they are taking a purely "top down" approach, "starting with principles, standards, stewardship, and data processing activities," and 15 percent said they are starting from the "bottom up," with data discovery and scanning data sources. Borlea did not recommend this approach: Given that the GDPR is significantly focused on the rights of data subjects, how do you go from scanning data sources to then understanding how that data is used? "There's a bit of a gap there," he said.

When asked what aspects of the GDPR they were focusing on first, 59 percent of respondents answered with the "data governance" aspect. This process involves understanding what data the company has, how that data is used, and where

data is stored.

Other responses cited included:

» Data-protection/privacy-by-design/data-privacy-by-default (25%);
» Accountability/data stewardship (11%); and
» Operational/responding to data subject rights (5%).

The GDPR introduces a legal accountability obligation. "My approach would be to start with accountability," Borlea said. "Build the organizational structure in such a way that it enables accountability, enables transparency, and everything then flows from data."

Article 24 of the GDPR, which codifies the accountability obligation, requires the implementation of "appropriate technical and organizational measures"—including by introducing data protection by design and by default principles where relevant—to ensure, and be able to demonstrate, that data processing is performed in compliance with the GDPR and that those measures are reviewed and updated where necessary. Documenting is essential. "What regulators will want to see in case of an audit is that the company can demonstrate accountability," Borlea said. "Documenting is key to how you demonstrate accountability."

Other ways of demonstrating accountability may be to provide the results of the company's data protection impact assessment and appointing a data protection officer (DPO) with clear roles and responsibilities. "These elements together will demonstrate accountability," Borlea said. "It's being able to demonstrate coverage of each of these aspects."

Some will be required to appoint a DPO independent from the firm whose tasks will include, in part, "awareness raising and training of staff involved in the processing operations," the GDPR states.

Many companies are still on the fence about appointing a DPO, however. The survey found that 46 percent of respondents said that they intend to, while 40.5 percent said they were unsure. The remaining 13.5 percent said they were not going to.

For those that intend to hire a DPO, keep in mind: Some articles of the GDPR leave room for interpretation locally within the EU. Thus, if the company has multiple entities across the European Union, Borlea recommends having one DPO for each jurisdiction.

GDPR ownership. Respondents were further asked who has overall responsibility for GDPR compliance. The plurality of respondents answered security/compliance (45%). Another 34 percent said legal, and 21 percent said IT.

A variety of other open responses highlighted the myriad ways that companies plan to oversee GDPR compliance. "We have put together a stream, compromising teams from IT, legal, security, and compliance/risk," one respondent said.

Another respondent noted that "legal and IT governance are managing the project with business operations sponsors." And a third respondent said his company has an "overarching project manager with two work streams: One arm is HR leading the people data with partnership of IT, legal, and risk management. The other arm will focus on the client data aspects."

Firms ignore the HR aspect of GDPR compliance at their peril. GDPR is about protecting data privacy rights of not just customers, but also employees, "so it's very important to involve HR, as well," Borlea said.

Ensuring GDPR compliance means having to address the following four closely linked pillars:

» **People:** You need to be able to capture people's roles and responsibilities and drive ownership to demonstrate accountability across the board.
» **Process:** Manage and provide a comprehensive view of your processing activities manipulating personal data, and demonstrate a clear audit trail for on-boarding new processing activities.
» **Technology:** Understand lineage and gain impact analysis capabilities: What is it linked to? Where does it go? How is it used?
» **Data:** Understand your data through the lens of GDPR by contextualizing it with specific attributes (e.g., risk level, retention period, applicable policies). Have the ability to easily find personal data using GDPR tags. Ensure you have the right information by involving the relevant owners and stakeholders.

The challenges posed by implementation are many. "GDPR will require an ongoing effort," Borlea stressed. It will require a shift in company culture, putting in place an organizational structure in which using personal data responsibly and transparently becomes woven into the fabric of the organization. ■

"The GDPR is not just about data protection, as its name suggests; it's about protecting the rights of data subjects."

Tudor Borlea, Sales Engineer, GDPR Specialist, Collibra