PREPARING FOR GDPR

GDPR will have a major impact for companies worldwide that manage the private information of European citizens. This market focus survey looks at the status of US companies' preparations for GDPR, their priorities and compliance expectations. Danny Bradbury reports.

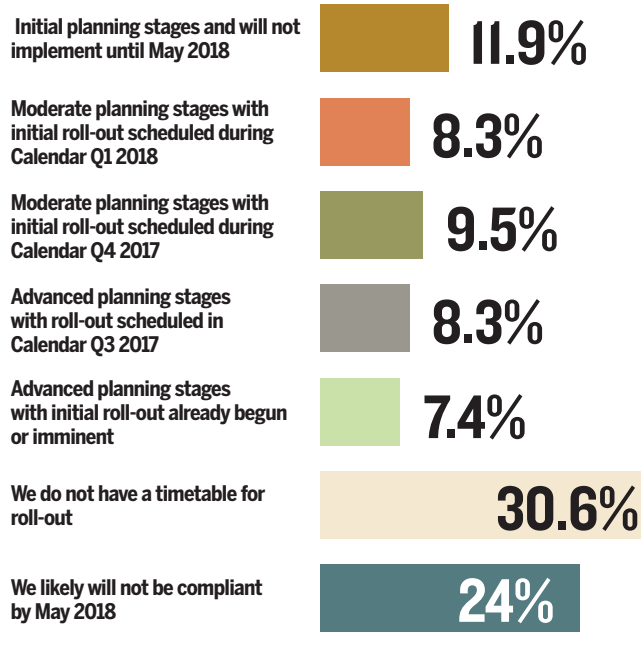
The General Data Protection Regulation (GDPR), which goes into force in May 2018, increases privacy requirements for companies dealing with sensitive personal data of European Union citizens. The regulations, which has worldwide ramifications, significantly changes how data is handled and the controls companies put over such manipulation of private data, with potentially massive fines for those who fail to protect the data effectively.

SC Media surveyed 337 IT and security professionals in the U.S. that do business in the EU and who access such private data to see how they planned to implement the new regulations. The survey, done in conjunction with C.A. Walker Research Solutions of Glendale, Calif., was underwritten by Guidance Software.

One resounding message that came back from the survey is that companies simply are not prepared for GDPR and, in fact, many are not aware of its ramifications.

As a regulation, GDPR has a significant legal difference to the mandate it replaces: the 1995 Directive 95/46/EC (often known as the Data Protection Directive). Directives are broad guidelines from the EU, and individual member states must implement them in national law. This can take several years from a directive's enforcement date. Conversely, regulations from the EU come into effect at once in each member state. National governments need not take any actions to install EU regulations. That said, GDPR will not be identical in every country. The regulations do provide for some flexibility for countries to interpret the rules differ-

GDPR Compliance begins in May 2018. Where is your company overall in planning and implementing GDPR? (Q6)



ently based on local laws and regulations.

An important item to note is that GDPR is often mistakenly cited as the replacement of the Safe Harbor rules. Safe Harbor is separate to the directive. The directive governs EU member states. Safe Harbor was a bilateral adequacy agreement between the EU and U.S. While GDPR replaces the directive, Privacy Shield replaces Safe Harbor.

William Long, a partner at legal firm Sidley Austin, who leads the firm's EU data protection practice, explains that this leaves companies without much room to maneuver. "There is no grace period," he reminds us. "There is no second chance."

This applies as much to North American companies and others worldwide as it does to European firms. GDPR is a European regulation, but it covers anyone storing data about EU citizens. U.S. companies dealing with individuals across the ocean will also be subject to its rules, as will the supply chain of U.S. companies that process this data, regardless of where they are based.

"Organizations should understand that GDPR compliance is not a single tool or change in process, but rather a culture of privacy that places personal data at the forefront of security and design," says Anthony Di Bello, senior director of products at Guidance Software. "It is an entirely different way of proactively viewing data collection, processing and storage that ensure the best possible controls are in place to mitigate personal data risk."

Under the new rules, companies must minimize the data they collect, limit its retention to a specific expiry date, and give consumers access to it – even going so far as to export the data in a machine-readable format so that individuals can take it to other service providers.

Other requirements include collecting consent to use data for specific purposes rather than relying on a blanket written agreement. Companies must also erase data on request.

Drivers for GDPR compliance

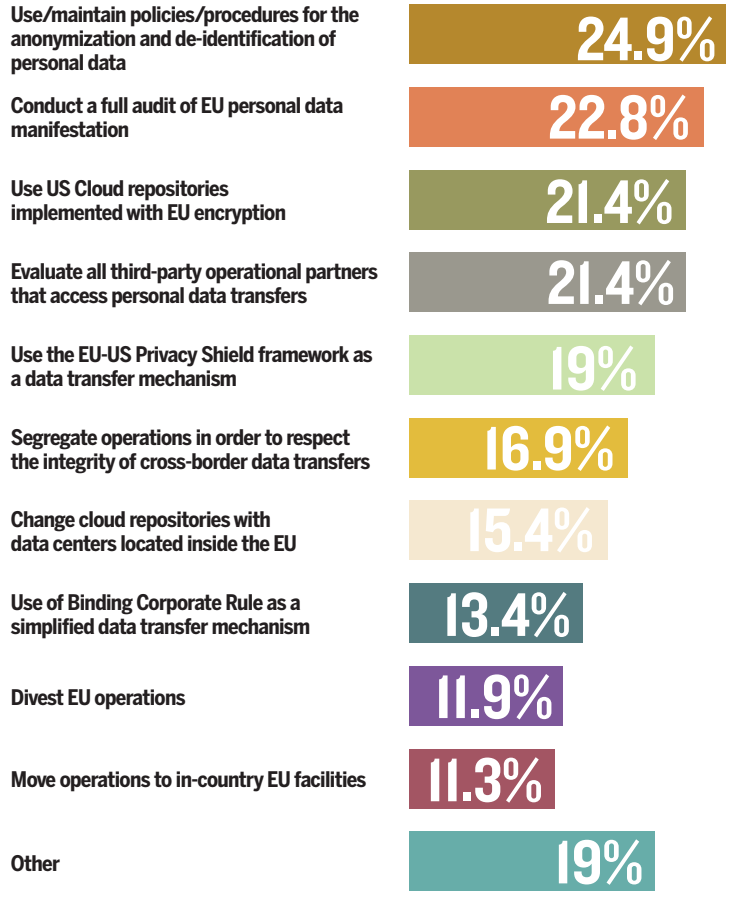
Many companies are unaware of the potential impact if they do not comply with GDPR. Financial penalties will be far greater under the new regulation than under previous rules. Regulators can fine violators up to €20 million or up to 4 percent of their global revenue, depending on the nature of the violation.

In spite of these unprecedented penalties, 42.1 percent of respondents to the SC Media survey say that it is no different from any other rule. That's a mistake, says Di Bello, who says that it could pose an existential threat for many companies. "Target recently settled its 2013 mega-breach for $18.5 million, but this figure could be well above $2.5 billion under GDPR," he says.

SC Media's research shows that cost is the priority when it comes to compliance. A quarter of U.S. respondents (25.4 percent) will follow the regulation that has the least impact on their bottom line. Companies want to tick the necessary boxes and reduce regulatory risk, but they are missing a big opportunity, according to Di Bello.

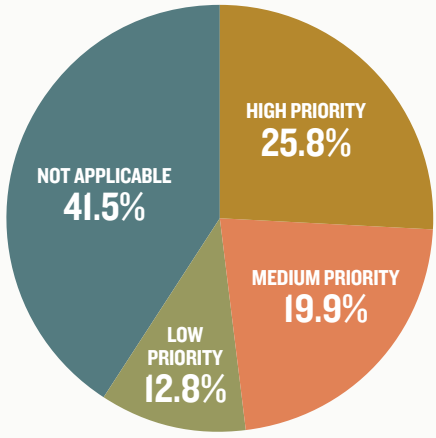
"While an upfront

In order to be operationally compliant with GDPR, we plan to do the following:

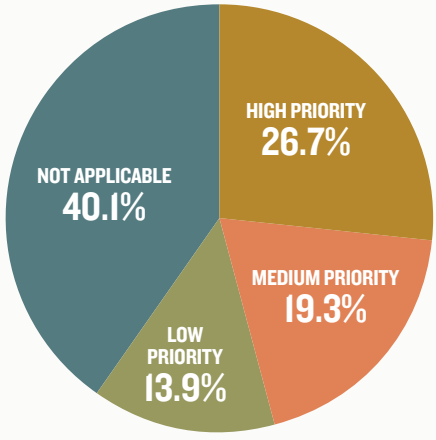


Prioritize the actions you need to take before GDPR goes into effect:

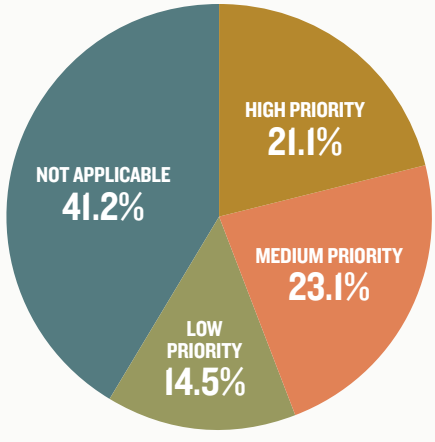
Establish a track record of compliance before the formal GDPR effective date



Institute a process of analyzing the risks that apply to EU personal data



Evaluate and implement technologies to achieve compliance with the GDPR's security requirements



investment in privacy fundamentals may bring about better compliance, there are competitive advantages that can also be realized," he says. "When organizations respect and enforce a culture of privacy, customers will take notice."

A preoccupation with immediate financial costs distracts businesses from the chance to use privacy and security as a selling point to build revenue, he warns. Only 17.3 percent of U.S. respondents to the survey prioritized compliance with regulations that increased corporate security, and only 15.2 percent put citizen privacy at the top of their list.

How prepared are companies for GDPR? Not very, says Ann Cavoukian, former privacy commissioner for the province of Ontario and now executive director at Ryerson University's Privacy and Big Data Institute.

"In the U.S. they don't understand what a game changer it's going to be," she warns.

The numbers bear out her concerns. Of respondents to SC Media's research, roughly one in five had completed no planning at all for their GDPR-related tasks. For some tasks, such as ensuring their firm could produce data on request in compliance with GDPR's 40-day timeline, that figure increased to almost a quarter (23.9 percent).

In spite of this slow start, some companies still believe that they will be ready. Only 10.7 percent said that they would not be in compliance by the deadline, May 25, 2018. In spite of this, almost one in five (19.3 percent) of the respondents admitted that they did not even have a timetable for rolling out their GDPR project.

Companies already compliant with the UK's Data Protection Act will have a headstart when it comes to compliance, but many will not have this advantage, warns Di Bello. "It appears these organizations have severely underestimated the complexity and time required for GDPR compliance," he says. "Underestimating the complexity and timeline of GDPR may be a result of misconceptions about the rules and general unawareness."

Companies that have prepared themselves are generally more mature ones, suggests Gabriel Voisin, senior associate specializing in in privacy and data protection at UK-based legal company Bird & Bird LLP.

"Often these are in regulated industries, such as financial services, and life science/health care organizations," he says. "These two, being so related, have identified ahead of the rest the importance of compliance with GDPR."

Again, the SC Media numbers support this view. Some 80.3 percent of businesses with more than $1 billion in revenues (49 of 61 companies in this category subset) already had their GDPR projects underway, compared to 71.9 percent of small to medium business with less than $100 million in revenues (46 of 64 companies in this subset).

The level of preparation is significant here as a quarter of the smaller businesses (16 of 64 companies) were still in the early planning stages, and didn't plan to complete implementation until May 2018, compared to just 13.1 percent of the larger companies (8 of 61 companies). Almost one in five companies with revenues of $1 billion or more (19.7 percent, or 12 of 61 companies) were through the planning stage and had begun their initial implementation, compared to just 6.3 percent of the firms with revenue of $100 million or less (6 of 64 companies).

SMBs might be at a disadvantage due to immature compliance and/or information governance structures, says Di Bello, although these firms will often be dealing with simpler data structures.

"Without the technical controls in place to ensure compliance with GDPR, the next best option is to conduct an enterprise-wide self-reporting process to identify, map, and analyze EU personal data as it relates to GDPR," he says.

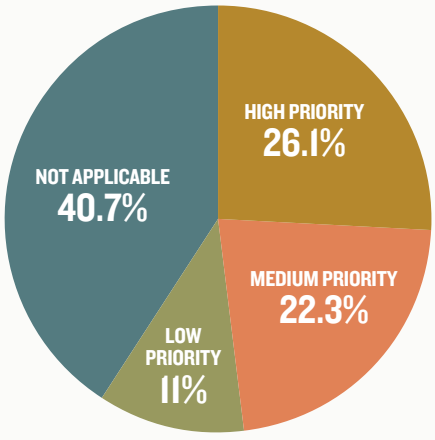
"The appointment or hiring of a data privacy officer (DPO) is mandatory and a good place to start to ensure key stakeholder buy-in at the C-level and with the board," Di Bello adds.

Priorities

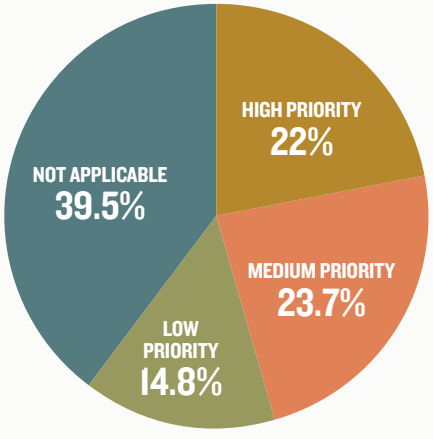
Some companies seem unworried about GDPR because they believe they have an easy solution up their sleeve: 14.2 percent of U.S. respondents to the SC Media survey say that simply divesting their EU operations altogether provides them with an easy get-out clause from the new regulations. That approach will not be as easy or as effective as they think, predicts Di Bello.

Prioritize the actions you need to take before GDPR goes into effect:

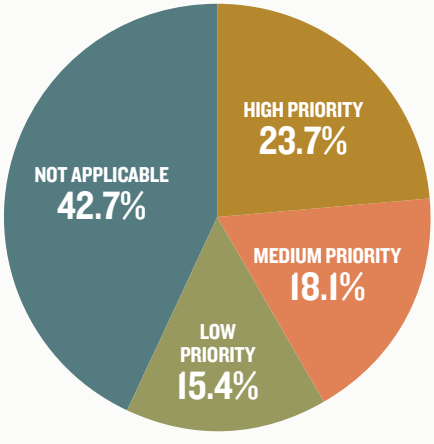
Review technology solutions for GDPR compliance and steps toward achieving compliance



Adopt a routine for maintaining documentation as it relates to the GDPR

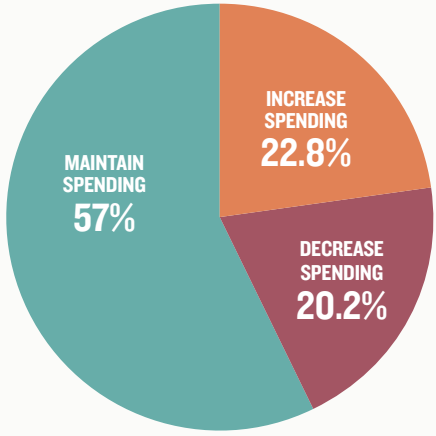


Recruit, train and appoint a qualified Data Protection Officer

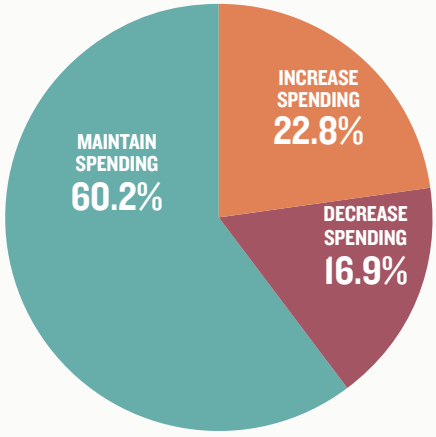


What are your budgetary technology priorities to ensure compliance over the next 12 months to address GDPR compliance?

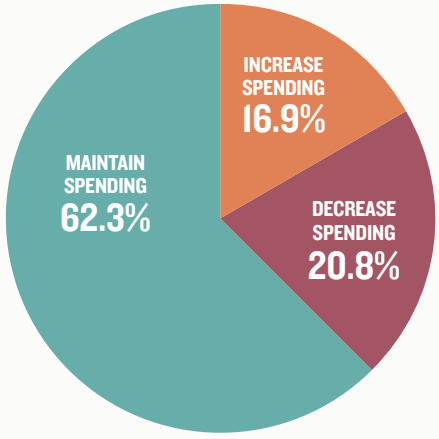
Data Classification tools



Governance, Risk, and Compliance (GRC) tools



Content Management Systems (CMS)



Companies handling any data belonging to EU citizens, even on U.S. soil, will still be subject to GDPR, he warns. "The level of effort required to completely sever all handling of EU personal data, whether directly or indirectly via EU partnerships, may be equal to or greater than GDPR compliance."

Many companies are committed to tackling GDPR head-on, though, and are focused on several priorities in their GDPR preparations. Four in ten of them (40.6 percent) say that developing a risk analysis process for their EU personal data was their highest priority. This is followed closely by the need to establish a track record of compliance before the formal GDPR effective date. Some 40.1 percent of companies label this a priority. An equal number highlight a review of technology offerings for GDPR compliance and the steps to achieve compliance (40.1 percent).

Technology will be a core tool in GDPR compliance, says Di Bello. "New technology is continually evolving and the area of proactive data security is growing," he says. "Organizations should regularly review spending priorities and should consider how existing and new tools support changing compliance and security needs.

He highlights some critical items that companies may want to include in their GDPR toolbox:

- File analysis
- Data classification tools
- Governance, risk and compliance (GRC) tools
- e-Discovery
- Enterprise information management (EIM)
- Mobile data management
- Collection tools
- Data loss prevention (DLP)

Investment

This raises the question of investment. Do companies anticipate increasing their investment to meet GDPR compliance deadlines? Which tools are they buying with that money?

Across the board, almost half of the respondents say they will maintain current levels of spending over the next 12 months, while just over a third plan on increasing their GDPR investment.

"Achieving strict and dexterous control over all GDPR-covered data often requires investing in more capable technology solutions than organiza-

tions currently possess," says Di Bello, pointing to Ponemon Institute figures that show non-compliance costing 2.65 times more than compliance.

"Such investments are certainly both necessary from a legal perspective and valuable from an ROI viewpoint," he adds.

Where they are investing, companies are focusing their efforts on a few key tools. Governance, risk and compliance (GRC) drew the greatest interest, with 35.5 percent of companies increasing spending over the next 12 months, and just 18.3 percent decreasing their investment.

Data classification tools were another popular category, with 36.5 percent of companies increasing their investment and 20.8 percent planning to spend less. This might stem from one of the biggest challenges that companies are experiencing with GDPR: labeling the data of EU citizens.

Long says that the first step in any GDPR program is to understand one's current status. "The first phase invariably involves some kind of data mapping," he says. "If you don't know where your data is, who has access to it and what systems it's on, there's no chance of you being able to do a GDPR project."

Classifying data is a particular challenge for companies grappling with GDPR. While just under a third of U.S. respondents (32 percent) have processes in place to identify data records from EU citizens, more than a quarter (26.4 percent) have yet to start working on it.

"The ability to systematically identify EU citizens' personal data across an entire enterprise will be incredibly challenging," says Di Bello, who points to a number of hurdles to compliance, namely data sprawl, shadow IT, remote workers and BYOD.

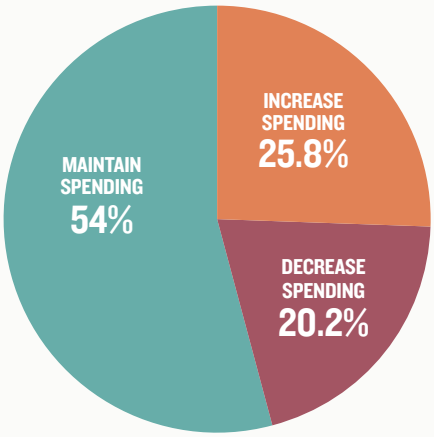
"Understanding the definition of EU personal data (i.e., even dynamic IP addresses can be considered personally identifiable information), ensuring that EU personal data is not transferred between countries during discovery, and maintaining compliance throughout the process presents a whole new set of challenges," he says. "Only with the help of technology can one even attempt to meet this requirement."

One silver lining is that GDPR standardizes the requirements, ensuring that the same rules apply across each country.

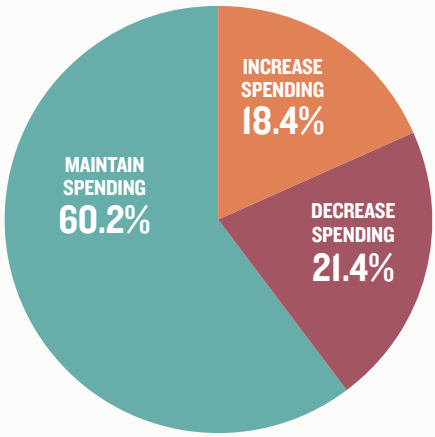
Part of the problem for companies exploring GDPR is that while the regulation itself is now well under-

What are your budgetary technology priorities to ensure compliance over the next 12 months to address GDPR compliance?

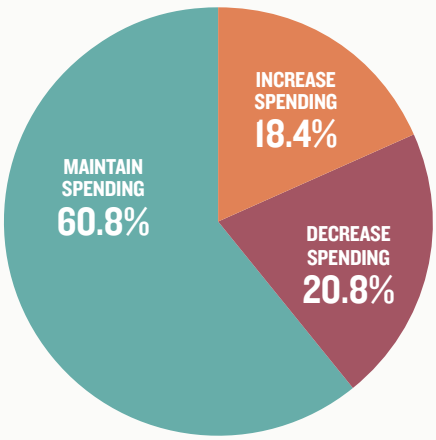
Data Loss Prevention (DLP)



Records Management (RM) products



Anomynization and de-identification tools



GDPR in the EU

Indications from research conducted by SC Media suggest that EU organizations are further along in their preparations for GDPR than their U.S. counterparts, having made progress in areas such as identifying data on EU citizens. The self-evident reason is that more companies in the EU are likely to have reached compliance in May 2018 than in the U.S., in part because virtually every company in the EU is likely to have a business relationship with another EU company.

Given the inescapable logic of that, there is plenty of work still to be done, according to Fortunato Guarino, EMEA cybercrime and data protection adviser at Guidance Software.

"To this day, many companies still tend to underestimate the risk of cyberattack and the subsequent costs in terms of remediation, reputation and regulatory compliance," he says, warning that companies not compliant by the deadline are assuming a significant financial risk. "Confusion regarding exactly how the law will be applied and enforced may also exacerbate the delay."

To become compliant with GDPR, evaluating relationships with third-party data processors was a priority for most EU firms, while another was developing techniques to de-identify data (a key component of Privacy by Design principles). De-identification is not an explicit requirement under GDPR, but the U.K. Information Commissioner's Office (ICO) has identified it as a potential technique to help companies meet the regulation's accountability principles.

U.K. companies, or those hosting data there, face yet another confounder when dealing with GDPR: Brexit. The U.K. is poised to leave the EU, although this would not happen until after GDPR comes into effect there. Nevertheless, this shouldn't tempt U.K. companies to forego GDPR compliance, Guarino warns.

"U.K. businesses should be GDPR compliant for the simple fact that so many do business in the EU," Guarino says. He adds that many of them have already started down that path and hired a data protection officer (DPO) to help them achieve compliance.

While SC Media research for the U.K. was nominal, two indications from a very small sampling of respondents confirms that hiring a DPO is indeed high on the list of priorities, as does establishing a track record for compliance. This latter point is important because the way the GDPR regulations are written, a company's effort to be compliant is taken into consideration if regulators need to determine if compliance is violated. In this regulation, a company's good intention to be compliant is important.

In any case, the majority of U.K. consumers are privacy-conscious and will want to see their information treated according to the same standards as citizens across the English Channel, Guarino points out.

This makes security a selling point for U.K. companies doing business elsewhere, he explains. "GDPR can be an opportunity for U.K. companies doing business in the U.S. By improving their information governance and customer privacy protections, companies can create a competitive differentiator that customers will notice."

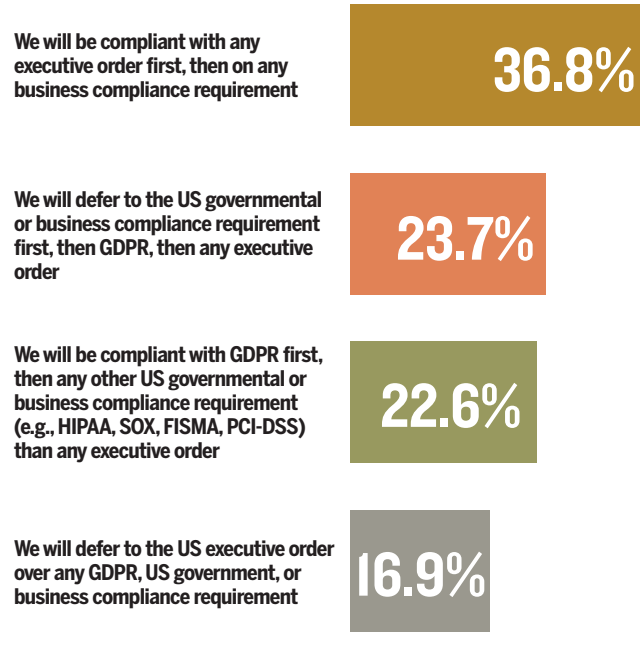
stood, the international legal landscape is shifting. Companies must cope not only with GDPR compliance, but with the process of transferring data in and out of Europe.

EU and U.S. companies exchanging data rely on adequacy agreements, in which they reach a consensus that their respective legal privacy frameworks match each other well enough not to cause any problems. GDPR raises the privacy bar in Europe, which experts worry could affect adequacy status elsewhere.

In January, President Trump signed an Executive Order that worried privacy advocates. Called Enhancing Public Safety in the Interior of the United States, it repealed privacy protection for non-U.S. residents under the U.S. Privacy Act, which deals with privacy provisions within the federal government. European members of the European parliament worried at the time that it could threaten an existing Privacy Shield adequacy agreement between the two powers.

This leaves U.S. companies deciding which legal framework to follow, should any inconsistencies develop between U.S. and EU law. Almost a quarter

How will the new U.S. Executive Order on the exclusion of non-US citizens from PII protections in US privacy laws impact how your company implements GDPR compliance?



of respondents (22.6 percent) say they would prioritize GDPR, and then follow U.S. governmental or business regulations after that, rather than an executive order. The remaining respondents were more likely to obey the executive order than they were a governmental regulation, such as Sarbanes-Oxley Act, or a Security and Exchange Commission regulation.

These legal machinations leave companies in a difficult position. If there's one thing businesses dislike, it's uncertainty, and yet nothing seems certain in cross-border privacy law today. How can they hedge against the unknown?

Standard contractual clauses are one way forward. European policymakers have long recommended boilerplate contractual text supported by U.S. law that makes it possible for companies to craft bilateral agreements on the exchange of data. Using such a clause, a European company can give data to a third-party service provider (in legal terms, a "data controller") in the U.S.

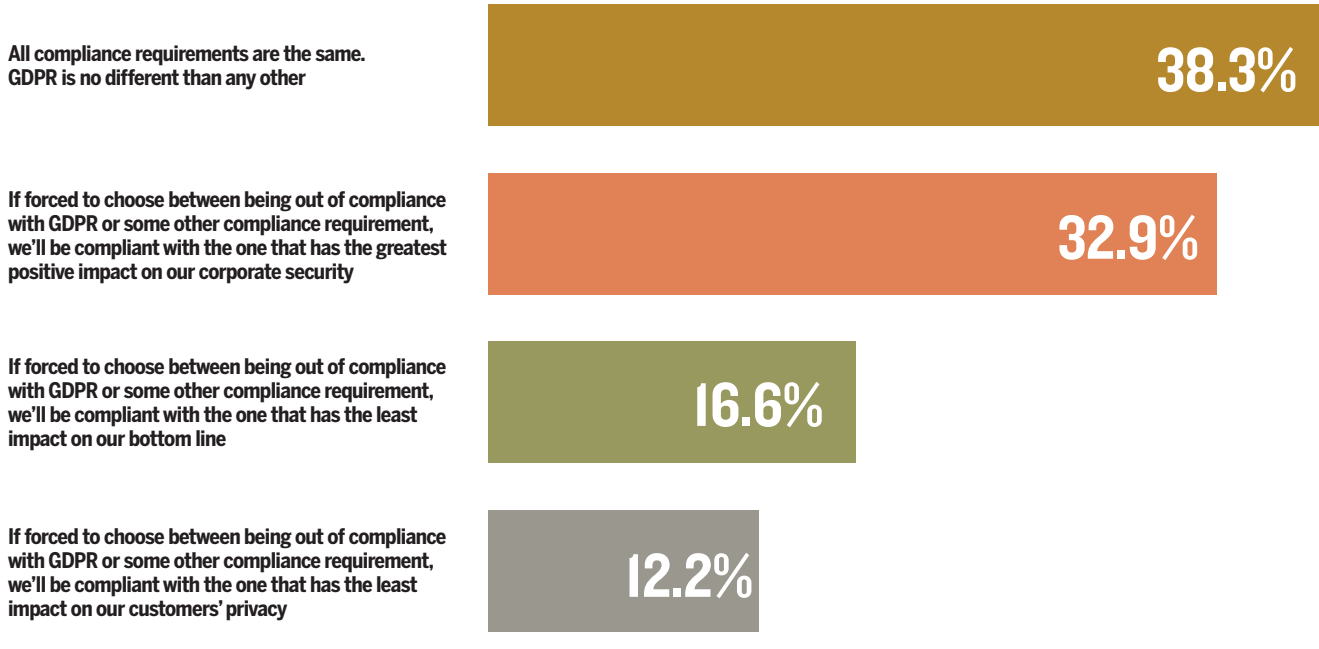
One point is certain: The longer that organizations take to start their GDPR programs, the more likely they are to need outside help. At the time of writing (June 2017), the enforcement date for this groundbreaking regulation is barely a year away.

Companies in the U.S. are limping toward GDPR compliance. And, as the deadline looms, there's every chance that they will require a mixture of technology tools and external help to get the job done. There's a lot of heavy lifting to do.

Methodology

This survey was based on 337 responses from a broad cross-section of company sizes and revenues and eight industry verticals, including federal and state and local government, technology services, finance, education, manufacturing, medical and health care, legal/real estate and retail and wholesale distribution. The survey was conducted in April 2017 by C.A. Walker Research Solutions, Glendale, Calif. The results of this survey might not equal exactly 100 percent due to the following reasons: rounding errors during the analysis phase of research; respondents who skip a question; and respondents who provide more than one answer to a question. This research has a confidence level of +/- 3.3 percent.

Penalties for non-compliance with GDPR can be substantially higher than other compliance penalties – up to 4% of worldwide revenue with a €20 million cap. Based on these very high penalties, how does GDPR compliance rank against other compliance requirements?



About Guidance Software

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, and EnForce™, an automated cyber risk management platform, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats.

From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 34 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

For more information, visit us at guidancesoftware.com