NAVIGANT

GLOBAL LEGAL TECHNOLOGY SOLUTIONS

BECOMING GDPR READY: REAPING REWARDS BEYOND JUST COMPLIANCE

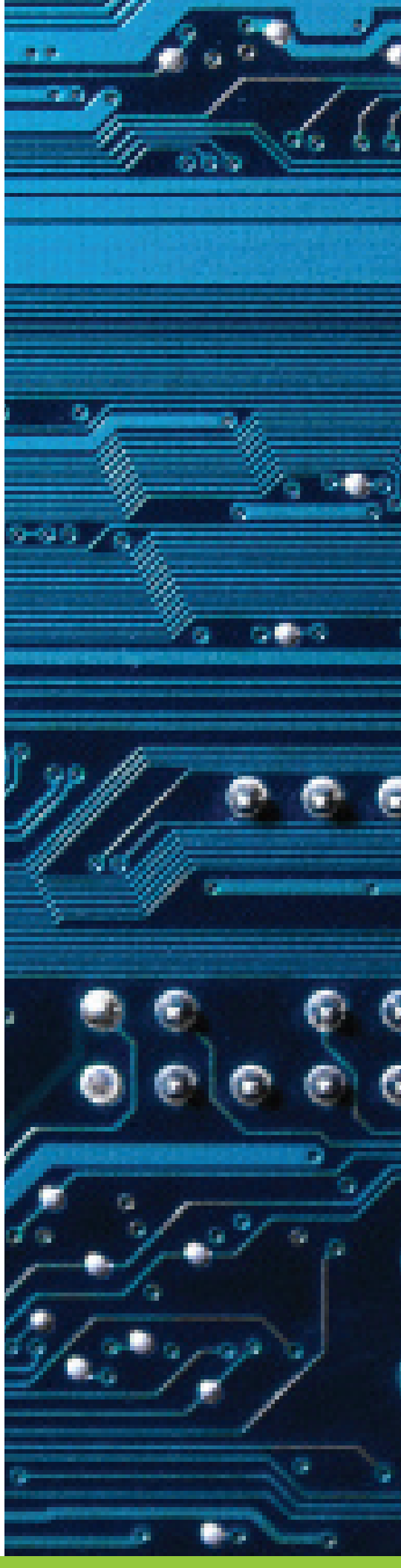
In May 2018, European Union authorities will begin enforcing strict new standards for handling the personal data of EU residents. Outlined in the new General Data Protection Regulation (GDPR), these standards will apply to businesses that handle personal data of individuals in the EU — even when no transaction takes place and regardless of whether a business is physically located in Europe. As a result, the complex new rules will apply to many more U.S.-based companies than did the previous standard. Hotels, universities, cloud-based businesses, and all organizations that market to an international base must take heed.

While a few U.S.-based organizations — mainly those with global operations — are already preparing to comply, others are unaware that GDPR exists. Still other companies are familiar with the new rules, but have decided to hold off on preparations while waiting for clarification on certain provisions and confirmation that the new rules will indeed apply to them. However, while GDPR will not apply to all companies based in the U.S., it certainly will apply to more than many realize.

Despite this uncertainty, a wait-and-see approach is ill-advised. GDPR will require any U.S. company that targets EU consumers to conform to a unified privacy regime that is very different from the U.S. sector-based laws currently in place. For those without a current model, building, testing, and deploying the sophisticated data infrastructures and security systems that GDPR demands — plus instituting new policies and procedures — will be a massive undertaking. Preparing internal processes and controls can take a significant amount of time for any company — and there will be no additional grace period once the law goes into effect.

Potential fines are severe for companies that violate GDPR, particularly if regulators find evidence of negligence, willful disregard for known compliance shortcomings, or harm to a large number of EU residents through, for example, a security breach. Companies that are found to have willfully violated the new rules could face fines of up to 4 percent of their prior year's global net revenue. For a U.S.-based company with $500 million in sales, that translates to a potential liability of $20 million.

Fines aside, by addressing the challenges posed by GDPR, particularly those around information security, companies can enjoy many broad business benefits. Building data inventories, conducting security assessments, and strengthening privacy protocols can bolster legal and compliance initiatives, as well as enhance a company's reputation. Even if certain companies do not need to comply immediately once rules are clarified, they may find themselves subject to regulatory bounds sooner rather than later. Many experts believe that GDPR has the potential to become a de facto global standard for data governance and privacy. Embracing these regulations now may very well translate into a competitive advantage down the road.



WHAT IS GDPR AND WHAT DOES IT MEAN TO YOU?

According to the European Commission, GDPR is "the most important change in data privacy regulation in 20 years." The Commission believes that the new law, which will replace the EU's 1995 Data Protection Directive on May 25, 2018, will reshape the way organizations across the region approach data privacy. There is also a distinct possibility that GDPR — and similar efforts to coalesce around a common scheme for data privacy — will eventually transform data privacy around the world.

For now, it is critical to note that GDPR rules apply to both controllers and processors. All downstream parties handling data must also follow GDPR if it applies to the original data-handling organization. Significantly, the concept of "processing" personal information includes a litany of actions, spanning from initially obtaining the personal data through internal storage and transfer and ultimately to any external transfer and deletion. GDPR enforcement will extend into all aspects of organizations, including cloud computing, social media, and the internet of things.

Some key features of GDPR include:

- **Breach notification:** GDPR requires organizations to notify the supervising authority of any data breach likely to "result in a risk for the rights and freedoms of individuals" in all member states. When feasible, organizations must notify authorities within 72 hours of becoming aware of the breach and provide sufficient rationale for their reasons if they do not provide timely notification. Similarly, they must also notify customers "without undue delay" after first becoming aware of a breach.
- **Consent requests:** The new rules strengthen consent conditions and require that individual consent requests are presented in plain language. They stipulate that all business partners must have easy access to the consent requests. In addition, when consent is obtained directly from the data subject, withdrawing it must be as easy as providing it.
- **Data subject rights:** GDPR also expands rights for data subjects to obtain personal information held by a company, request details on how that data is being used, and exercise the "right to be forgotten," among others. Data controllers face the obligation to erase all of a subject's personal data at his or her request.
- **Privacy by design:** The new rules call for "privacy by design" — the inclusion of data protection in the design of systems rather than as an afterthought.
- **Data protection officers:** Organizations that handle large amounts of data or certain types of data as a significant element of their business will now be required to hire a data protection officer (DPO). Among other rules, the DPO must report to the highest level of management and be provided sufficient resources to carry out the job and "maintain their expert knowledge."
- **Data Protection Impact Assessments:** Where a type of data processing, especially one using new technology, is likely to pose a high risk to data subjects, GDPR requires that an organization must carry out a detailed assessment of the impact of the anticipated operation on the protection of personal data before initiating the processing operation.

GDPR is designed to apply to all industries. Although the systems and safeguards required to meet GDPR could feel daunting to many U.S.-based organizations, they may seem familiar to organizations subject to information privacy requirements issued by the many government agencies that regulate sectors of the U.S. economy, including healthcare, financial services, and energy. Despite this familiarity, the sectoral nature of U.S. privacy regulation involves varied regulatory agencies at state and federal levels managing the privacy elements of different industries in different ways. GDPR's expansive scope of compliance requirements go beyond what many U.S. companies are required to adhere to today — or may be prepared to address in the near future. For organizations that have weak privacy or information security protocols in place or lack them altogether, compliance may prove difficult and complex. While the road to being GDPR-ready may look formidable for many organizations, the business and financial efforts required to comply are far outweighed by the risks and associated financial harms that could result.

Many experts believe that GDPR has the potential to become a de facto global standard for data governance and privacy.

HOW TO GET OUT IN FRONT OF GDPR

The cost to comply with GDPR may represent a significant investment, but companies can realize broad operational benefits from GDPR-related exercises such as creating data inventories, conducting security assessments, and building privacy protocols. At a base level, companies should be aware of the data they collect and its movement across the enterprise. A common issue uncovered by data inventories, for example, is the discovery of data that is not being actively utilized for any purpose. By ceasing to collect unnecessary personal data, companies can potentially mitigate risk and save resources. This consideration is important because, under GDPR, personal data can be collected only for a specific purpose, and further permission from the consumer is required to use data in ways that fall outside the original intention of the data collection.

Implementing policies and practices to address the challenges posed by GDPR provides tangible and long-lasting benefits that extend well beyond regulatory compliance. For example, by keeping up-to-date records on privacy policies, data, risks, and IT controls, organizations will likely see improvements in storage management, business continuity planning, and risk mitigation, as well as an overall reduction in their information security threat profile. Clear data classification and typing enables better disaster recovery and business continuity planning. Such investments toward GDPR compliance can thus produce multiple benefits.

While such measures may be enacted for GDPR compliance, the steps a company has taken to enhance privacy protections may be a selling point in the U.S. market. With so many recent security breaches at large, global organizations hovering in recent memory, the general public is far more aware and concerned about the protection of their personal information and should welcome news of heightened protections.

Leading an effective GDPR compliance and control effort will require cooperation among companies and their vendors, as well as among different business units within the enterprise. As with any change, companies must establish new governance structures — including program management infrastructure, organizational oversight, and reporting and communications — to steer and guide their initiative. The next steps are to build data inventories and conduct an information security assessment that includes a review of networks, devices, and IT infrastructure to reveal potential vulnerabilities. To meet GDPR criteria, companies must then take a close look at their privacy governance and policies, improve their consent protocols, and create channels to address requests from individuals regarding their data. Organizations should perform testing to ensure that all identified gaps are closed — including documentation and process gaps — or that a plan is in place to close all gaps before May 2018.

START NOW ON THE PATH TO GDPR READINESS

Compliance with GDPR will require much more than the flip of a switch. Full compliance will be required in May 2018, and the technology, corporate policy changes, and professional resources necessary to meet this standard could take a considerable amount of time, financial investment, and technical expertise not currently present in the business plan or related budget.

Should the assessed impact of GDPR be viewed as positive after going into effect, it is possible, if not probable, that it will have a global impact on the privacy landscape. As regions continue to evaluate enhancing and building their own privacy regimes, it is reasonable to expect international interaction might guide them to implement a similar set of standards, creating a more cohesive and globally aligned regulatory approach. So companies that embrace this process now may very well find that they have a broader global advantage in the not-too-distant future.

In sum, while the required effort may be considerable, the avoidance of potential risk and the varied long-term benefits achieved by an organization that proactively and comprehensively addresses GDPR compliance are considerable and worthy of prompt attention.

Preparing internal processes and controls can take a significant amount of time for any company — and there will be no additional grace period once the law goes into effect.

CONTACTS

DAVID MANEK
Director, Data Privacy
+1.312.583.6841
dmanek@navigant.com

COLLEEN YUSHCHAK
Director, Data Privacy
+1.202.973.2485
cyushchak@navigant.com

BRIAN SEGOBIANO
Associate Director, Data Privacy
+1.312.583.2749
brian.segobiano@navigant.com

LAURA VIVET
Managing Consultant, Data Privacy
+1.202.481.8369
laura.vivet@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

linkedin.com/company/navigant

twitter.com/navigant

©2018 Navigant Consulting, Inc. All rights reserved. 00006563

Navigant Consulting is not a certified public accounting firm and does not provide audit, attest, or public accounting services.
See navigant.com/Licensing for a complete listing of private investigator licenses.