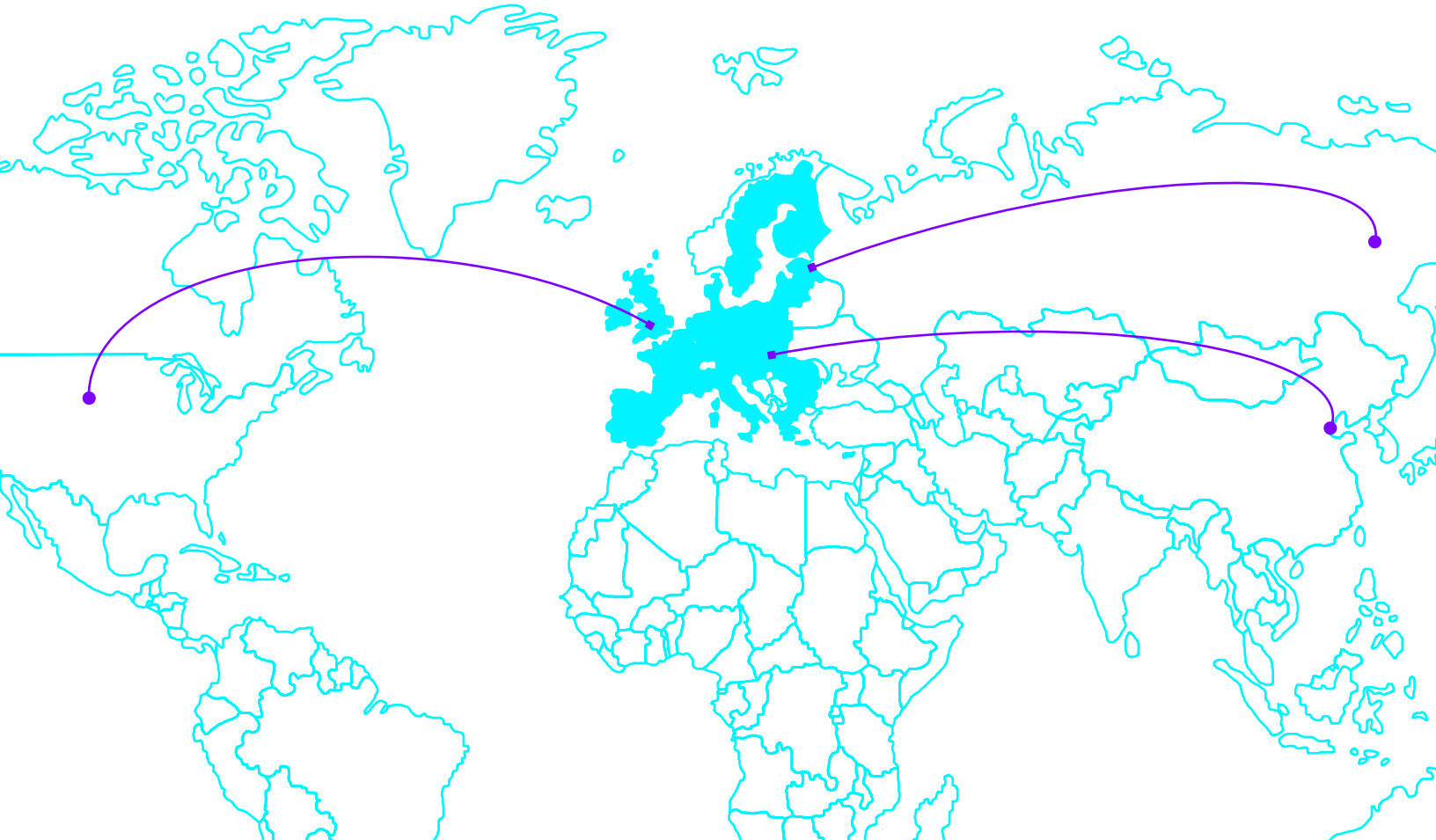

accenture
GDPR: THE TIME
TO ACT IS
NOW

The EU General Data Protection Regulation (GDPR) is considered the most important change in data privacy regulation in 20 years.[1] It has substantial ramifications for tech companies not just in the EU, but globally (Figure 1).

Figure 1. An EU regulation with far-reaching impact

GDPR protects all EU data subjects, independent of where they—or their data—are located



The regulation protects the data of all EU subjects regardless of the country in which they reside or the platform on which their data resides. If a tech company houses, handles or exchanges the data of any EU citizen it is required to be GDPR compliant.

GDPR will require strengthening of data privacy controls, enhancing of technology for management of personal data and the supplying of detailed documentation. For cloud suppliers and those companies who work with them, GDPR will also force major operational changes–so much so that it could slow both innovation and growth.

WHY GDPR IS DIFFERENT THAN PRIOR REGULATIONS

Regulations are always evolving and tech companies routinely manage regulatory changes as part of everyday operations. But, GDPR stands to have far greater impact than what tech companies have dealt with to date. Here's why:

There's a sharing of liability—In the past, data controllers (those who collect and use data) assumed responsibility for data protection. Now, for the first time, data processors (those providing data processing services, such as cloud services providers) will have direct compliance risk and obligation. Accountability for data protection cascades down through the data supply chain. Web-based companies will have to clearly define responsibilities and liabilities among solution partners, which could have significant implications across the organization.

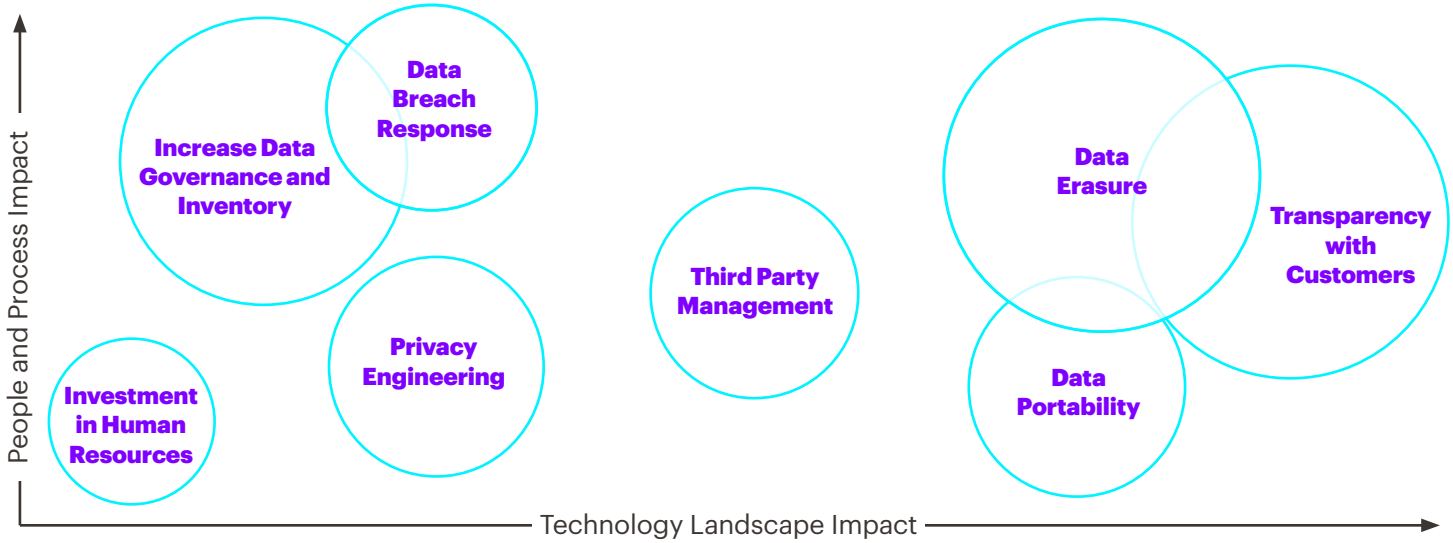
Most businesses are under-prepared—In the fall of 2016 customer perception of cloud services providers showed only 6% were believed to be compliant with GDPR without having to negotiate new contractual terms[2] and 91% of companies had concerns about their organization's ability to comply with GDPR, due to data processing complexity and costs.[3]

There are serious consequences—GDPR carries new and stricter requirements for capturing and managing personal information. It provides individuals with explicit rights that have implications for how tech companies manage consumer data across people, processes and technology. GDPR also has implications for consumer trust: 83% of respondents to the Accenture Technology Vision survey confirmed that trust is the cornerstone of the Digital Economy. Adhering to data privacy and security expectations as spelled out in GDPR is fundamental to maintaining consumer trust and protecting one's brand. And, non-compliance is not a viable option. GDPR significantly strengthens data protection enforcement and accountability and authorizes penalties for non-compliance of up to €20 million or 4% of global annual turnover, whichever is higher.

CAN YOU MEET THE REQUIREMENTS?

GDPR has eight primary requirements, some of which wreak more havoc than others on company operations and technology (Figure 2).

Figure 2. GDPR impacts people, process, and technology



The size and placement of the circles are indicative of the estimated magnitude of the impact on an organization due to GDPR regulations based on experience.

How ready is your company? To what extent can you demonstrate the answers to these questions?

Do you know where your consumer data is?
GDPR readiness requires that organizations know the attributes of the data they store and process in order to adequately protect it. Leading companies can trace 70 to 80% of this data to its source, today. Many companies are not as prepared. Even leading companies say getting an inventory of the last 20% of their relevant data will be tough.

Can you clearly demonstrate consumer consent?
GDPR requires that organizations provide individuals with concise and understandable notice of data collection and processing activities and that they receive clear consent from the individual to proceed. This has far-reaching impact. For example, a company can't use a person's information for marketing purposes, or even as part of contextual information about a customer segment, without that person's explicit permission.

Are your internal privacy controls robust and your products and services privacy-friendly?
GDPR requires that organizations integrate privacy controls into systems and processes that make use of personal data and that they provide consumers with products and services that automatically apply privacy-friendly settings. Right now, more than half (55%) of businesses are not confident they completely meet customers' data security expectations.[4]

Is the data you store portable and transferrable?
Organizations must comply with an individual's request to transfer personal information to them or another organization and do so in a format that is machine-readable. This takes many capabilities including the ability to structure data to be portable and manage data that is shared across multiple platforms or vendors. Tech companies will also need to engineer secure solutions that give consumers visibility to their data and the ability to select which data should be transferred.

Can you completely erase personal data when needed?
GDPR gives individuals the right to "be forgotten", meaning organizations must erase personal data if it is no longer needed or the individual withdraws consent. This requires having the technology and processes to find data across the organization, delete it from systems, inform third party processors of the erasure request and demonstrate compliance. Today 84% of cloud services do not immediately delete customer data on

Compliant or not?

Organizations are working aggressively to personalize the experience they offer customers. For many tech companies it is a standard process to gather personal information and use it to determine the best offer to share with customers as they traverse the digital landscape. Fast forward to June, 2018. Lori Smith asks Company ABC to be forgotten. Company ABC erases Lori Smith's personal data from its systems. However it had used Lori's personal data to develop personas to guide its decisions on the best digital ads to offer specific customer segments. Company ABC does not alter its personas to reflect the removal of Lori's data. Is Company ABC compliant with GDPR data erasure or not?

termination of contract.[5] Further, only 28% of IT and business decision makers even realize the right to be forgotten is part of GDPR.[6]

Can you quickly recognize and report a data breach?
In 2015, one billion customer records were leaked. Another billion accounts were hacked in just one breach in 2016. GDPR gives individuals the right to be notified quickly if a breach occurs by requiring organizations to report data breaches to data protection authorities within 72 hours. Today, only 1% of cloud services provide notification of security incidents in fewer than 24 hours.[7]

Are you confident that the third parties you utilize will be GDPR compliant?
GDPR defines accountability for data protection across the data supply chain. Web-based companies will have to clearly define responsibilities and liabilities among solution partners. Solution partners for data processing activities create liability for both the third party and the organization hiring that third party for services. With 9 in 10 organizations reporting they are concerned about their ability to comply with GDPR,[8] the liability risk is high. It will require tech companies to define roles, responsibilities and liabilities among parties and have expertise in legal contracting, vendor management and risk management to create new constructs for engagement between platform partners.

Are you fully staffed with skilled privacy practitioners?
GDPR readiness requires organizations to invest in privacy personnel and employee training and establish processes that provide increased collaboration across business functions. Key privacy positions must be filled and staff training must be developed to meet the compliance requirements of GDPR. For companies processing large amounts of sensitive data, this may also require appointing a Data Protection Officer.

Liable or not?

A retailer runs its ERP in the cloud. The ERP provider hosts its application on a cloud platform and the solution includes a third-party plug-in for ecommerce payment processing. In September 2018 the retailer has a data breach. Does liability under GDPR fall on the ERP provider or are the cloud infrastructure provider and ecommerce plug-in provider also liable for the breach?

WHAT TO DO TODAY

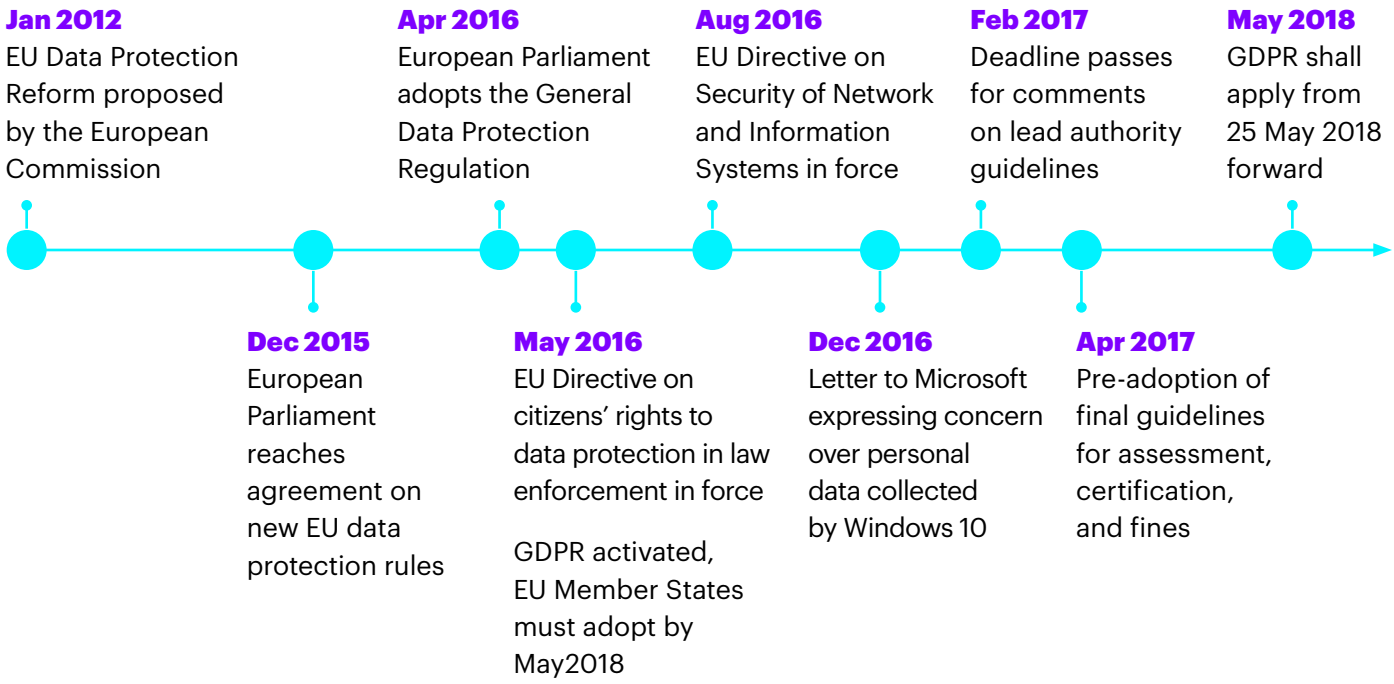
It can be an onerous effort to implement the people, process and technology changes for GDPR compliance. The countdown toward GDPR has begun and every day matters (Figure 3). At this stage, more than 50% of businesses think they will be fined once GDPR becomes enforced.[9] Here are three immediate actions to take to push you forward.

Determine your internal compliance strategy for GDPR. As this regulation is applicable to EU Data Subjects it will cross borders and operating lines.

Once you've determined your strategy, assess how your operations measure up. Evaluate your internal capability to execute GDPR requirements. To move quickly, consider getting an external assessment that is tailored to a company's specific compliance ambition and business scope.

Determine your best approach for trusted vendors and partners in data processing. Given the compliance risks of the extended data supply chain, you may consider enabling your compliance strategy with outsourced operations to minimize risk.

Figure 3. Timeline milestones



To learn more about how to determine your best compliance strategy, assess your GDPR readiness or execute your GDPR roadmap contact:

Kevin Collins
Managing Director
kevin.j.collins@accenture.com
+1 650 303 4633

Mark Egner
Senior Manager
mark.egner@accenture.com
+1 425 766 0886

NOTES

1. www.eugdpr.org

2. GDPR Analysis of 20,000 Cloud Services in September 2016 by Skyhigh Cloud Security

3. "State of European Privacy Survey," October 2016, Symantec Security

4. "State of European Privacy Survey," October 2016, Symantec Security

5. GDPR Analysis of 20,000 Cloud Services in September 2016 by Skyhigh Cloud Security

6. "State of European Privacy Survey," October 2016, Symantec Security

7. GDPR Analysis of 20,000 Cloud Services in September 2016 by Skyhigh Cloud Security

8. "State of European Privacy Survey," October 2016, Symantec Security

9. "Data Privacy Laws: Cutting the Red Tape," Ovum Market Research

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.