PATHFINDER REPORT

Essential Steps for Enterprise GDPR Compliance

AUGUST 2018

COMMISSIONED BY

TATA COMMUNICATIONS

About this paper

A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
(Ground floor)
30, Artillery Lane
London, E1 7LS, UK
P +44 (0) 207 426 1050

BOSTON
75-101 Federal Street
5th Floor
Boston, MA 02110
Phone: +1 617.598.7200
Fax: +1 617.357.7495

Introduction

The introduction of the European Union's (EU's) General Data Protection Regulation (GDPR) means that enterprises doing business in or with European countries must give careful consideration to their compliance, security and data privacy operations. Some enterprises will have already had strict data governance controls in place, but a large number will still be at the start of their data governance – and GDPR – journey. This report provides guidance on how organizations should go about preparing for GDPR by focusing on best practices around data governance and identifying tools and techniques that can also bring wider business benefits if implemented well.

KEY FINDINGS

- The EU's General Data Protection Regulation highlights the shifting attitudes about data not only in Europe, but around the world. The regulation has global implications and is likely to stand as an exemplar for governments (and even some industry bodies) seeking ways to better protect their citizens' data and reduce cyber risk. If enterprises approach GDPR the right way, they can ensure they are in a better position to comply with other incoming regulations, while realizing benefits for the organization beyond GDPR compliance, such as more sophisticated use of data and better security controls.

- Many laws and industry regulations already require enterprises in vertical sectors like healthcare, financial services or retail to safeguard customer information and implement technology controls to protect personal data, so some organizations will be more advanced in terms of their GDPR journey than others. However, studies show there are still many multinational corporations (MNCs) doing business or seeking to do business in Europe that have not yet assessed GDPR compliance requirements. Around one-third of US-based MNCs polled by 451 Research about GDPR believe it will apply directly to their business, yet one-quarter of MNCs have done little as yet to identify the impact GDPR will have on their businesses or on their customers' businesses. With GDPR implemented in May 2018, these companies are late in assessing GDPR requirements.

- GDPR implementation presents a number of complex challenges around technologies and processes for many large organizations. Many will require help. Country-specific Data Protection Authorities and industry bodies will offer guidance, and service providers will also provide a wealth of information – with many having already undertaken their own GDPR compliance programs. We expect GDPR to be a focus of discussions between many MNC executives and their network, cloud and managed service providers. Indeed, some 23% of companies with headquarters in Europe now consider the capability to provide an in-country presence for the purpose of GDPR compliance as being a key requirement in their selection of a service provider or systems integrator partner.

- GDPR compliance is not a Europe-only issue. As many as 28% of MNCs with headquarters in the US see the need to meet compliance obligations regarding data sovereignty and GDPR as one of the most important goals for their IT departments in the coming 12-24 months. Those companies that have not started implementing policies, technologies and practices for GDPR should start immediately with a GDPR plan and roadmap.

Implementing Best Practices for GDPR

Security and compliance have always been of the highest importance to enterprises operating in highly regulated industries, but in recent years shifting governmental attitudes about the protection of personal/citizen data around the world have placed a new emphasis on how all companies store, process and use this type of information.

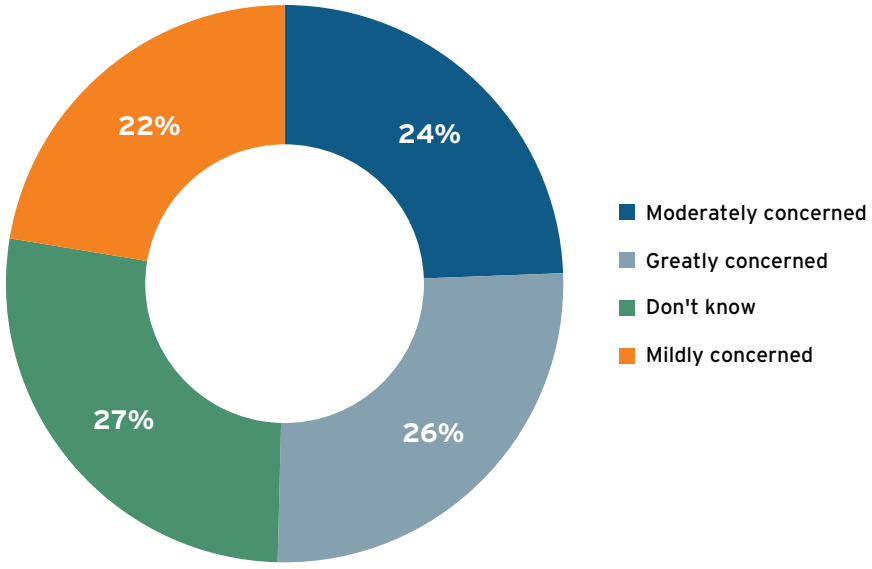
The EU's General Data Protection Regulation, introduced in May 2018, is a prime example of shifting attitudes around data use today. The regulation touches every organization that does business in or with the EU, and hundreds of millions of citizens. It places stipulations on how companies handling the data of persons in the EU or EU-based companies can gather (with consent) personally identifiable data, as well as how they can use that data (with carefully considered controls and permissions) and secure that data (with the right to retention and overseeing risk). It also places the usage rights of that data into the hands of the consumer (creating new requirements for data portability, among other things). While many compliance mandates are vague in terms of both prescriptions and penalties, GDPR, like PCI before it, has real 'teeth' in the form of hefty fines for noncompliance. Failure to comply could cost enterprises either €20 million or 4% of annual global revenue, whichever is highest.

Enterprises that want to avoid such risk will be required to prove they have a solid understanding of the concepts around GDPR and plans in place to become compliant. That said, much of the regulation so far is being left somewhat open to interpretation. This is why it is highly recommended that enterprises that have not done so already start creating a 'privacy by design' strategy around GDPR that allows the organization to identify the efforts required for compliance and to validate these efforts as they gain further understanding of the specific requirements of GDPR.

For some organizations, there is a sense of urgency. While nearly 40% of US-based MNCs surveyed by 451 Research in Q1 2018 said security and compliance are a 'critical and first consideration' for all new IT and business projects – and a similar percentage said these were of 'high importance' – as many as 27% of the organizations surveyed admitted to having done little to identify the full impact of GDPR on their business or their customers' businesses (see Figure 1).

Figure 1: Executive Views on the Likely Business Impact of GDPR

Q. What is your overall sentiment towards GDPR? (N = 250)



Source: 451 Research

For enterprises where GDPR preparations still need to be formulated, it should be noted that, when approached correctly, GDPR compliance could deliver benefits well beyond the assured protection of personal data. As companies implement data governance, they can also pave the way for better use and control of secure business intelligence and business data, as described in the next section.

WHAT IS PERSONAL DATA?

Under the GDPR, personal data is defined as any information relating to an identified or identifiable person. It can cover the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Examples of such data include:

- Identity information such as name, address and ID numbers
- Web data such as location, IP address, cookie data and RFID tags
- Records of products or services obtained
- Information on family, lifestyle, social circumstances (if it can be used to identify a person)
- Information on education, employment status
- Health data
- Biometric or genetic data
- Racial or ethnic data
- Political opinions
- Sexual orientation

Thinking Beyond GDPR Compliance

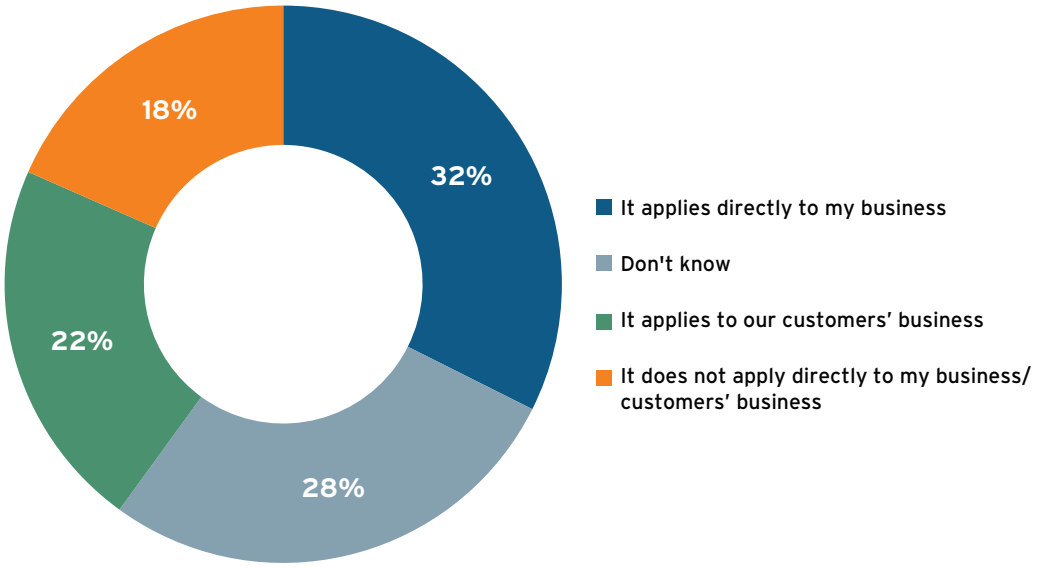
Enterprises are operating in a world where the balance of power is shifting toward the customer. Not only are customers concerned about how their personal data is used, they are more focused on overall customer experience. This means many enterprises are caught between the requirement for secure, solicited use of data and its more widespread use for business intelligence (partly to improve customer experience).

A growing amount of data is being harvested from websites, smartphones, connected TVs, gaming consoles, websites, point-of-sale systems and basically every digital consumer touchpoint. The amount of data exploited by businesses is also growing, and in many cases for MNCs, this is happening across geographic boundaries. As we use data more, the risk of infringement on privacy grows. Over the past few years, we have seen increased customer willingness to share personal data in return for some thing or service of value, however, and this is in part why governmental agencies such as the EU believe the time is right to ensure that appropriate protections are in place.

Of those MNCs surveyed by 451 Research, only 18% said they believed GDPR would not affect their business at all. One-third said it would have a direct impact, and just over 20% said it would affect their customers' businesses (see Figure 2). For many of these organizations, GDPR is driving a necessary expansion of operations and IT estates either into or across EU member states, so they can ensure that data is processed and stored 'in region' and in accordance with GDPR mandates.

Figure 2: Executive Perception of GDPR Impact on Their Own and Customers' Businesses

Q. Do you think GDPR will apply or impact your own, or your customers' business? (N = 250)



Source: 451 Research

Organizations globally are dealing with an explosion in both structured and unstructured data, and what regulations like GDPR call for is a strong information governance (IG) culture. Enterprises will first need to establish a clear data inventory and map of their data, and also provide an audit trail of its origins, storage and use. This could include data that is not digitized. They should also be able to track and trace the data, identify which databases within the application estate hold personal data, and then ensure that these comply with regulations.

While this work needs to be done for GDPR compliance, it can then be leveraged for other purposes, as the basis for creating new capabilities. This is because once you understand the true state of customer data, the business can use the information for building new revenue models and campaigns, creating more personalized products and services – while still complying with regulations.

GDPR compliance covers residents of all member EU countries. It restricts the free movement of personal data outside EU boundaries. It is required if the business has:

- A presence in an EU country.
- No presence in the EU, but the company processes personal data of European residents.
- More than 250 employees.
- Fewer than 250 employees, but its data-processing impacts the rights and freedoms of data subjects, is not occasional, or includes certain types of sensitive personal data – effectively this means almost all organizations.

GDPR CHALLENGES AND PAIN POINTS

Many laws and regulations already require organizations to safeguard customer information and implement technology controls to protect personal data, so it is natural that some organizations will be further along on their GDPR compliance journey than others. If your organization hasn't started yet, we suggest you first focus on building up a level of understanding across your business regarding its operations, the data it uses, and how GDPR will apply to different parts of the organization and different data types.

You will need to consider actively planning for new technology and process implementations, as well as ongoing risk assessments and support. Your organization will also need to think about its approach to data sovereignty, data in transit, security, and the tools and services that can be implemented to help ensure compliance with GDPR. Many companies will also need to consider skills – successful implementation of a GDPR policy will require the right skills, which we will discuss later.

Four Steps To GDPR Preparedness

STEP 1: PLAN - ESTABLISH A STATE OF READINESS AND PROVE YOU ARE PREPARED TO ACT

The European Union – and, we expect, individual country Data Protection Authorities (DPAs) that will oversee GDPR – will be reasonable regarding GDPR policing upon its introduction. However, we expect that as early cases are raised and go before the courts, and fines are issued, there will be increasingly greater clarity around what each requirement under the GDPR actually means when applied by law.

Information so far received from legal teams dealing with GDPR issues is that the courts are much more likely to be lenient in cases where companies can demonstrate that they have a plan in place – or a roadmap at least – for GDPR compliance. For this reason, organizations that have not done so already need to approach GDPR planning with a sense of urgency. If in doubt, seek guidance from local DPAs as well as the service providers you are working with, and leverage internal legal teams to develop forms of guidance that will provide the necessary understanding of GDPR requirements and how these will affect your organization. Remember, GDPR will also affect your service providers and the everyday working scenarios of your staff.

Everything organizations do going forward must be focused on 'privacy by design' – an approach that includes data protection considerations from the onset of system design, rather than as an addition or afterthought. This applies to building new IT systems for storing or accessing personal data, as well as developing new policies and using data for new purposes.

Under the GDPR, an organization will be either a 'controller' or a 'processor' of data. In many cases, they can be both – and in some cases, the organization's service provider will also assume some of this responsibility.

A Controller is: a person or organization that determines the purposes and means of the processing of personal data.
A Processor is: a person or organization that processes personal data on behalf of the controller.

Under the GDPR, organizations that carry out systematic processing of data subjects, or those that process large amounts of sensitive data (or data relating to criminal convictions or offenses) as part of their core activities are required to nominate a company Data Protection Officer (DPO). DPOs are required to have "expert knowledge of data protection law and practices" and an understanding of their company's data processing operations. Organizations are also asked that the DPO does not determine the purposes and means of processing data, so that they can provide independent advice. These DPOs will also be responsible for implementing internal records requirements, and for many companies they will be integral in identifying internal stakeholders, from marketing to sales and operations (where personal data is handled), and for placing appropriate checks and controls on the aspects of the business that must comply with GDPR.

DPOs should be the first point of call for drawing up a GDPR plan and putting a roadmap in place. They will find themselves working in a number of different phases, depending on organizational/technical maturity, and this work may vary from department to department. Conducting a maturity assessment should be a starting point for all DPOs and organizations looking to address GDPR so as to set the right goal and have a solid understanding of where the business is in relation with GDPR compliance today. A DPO needs to identify any former work undertaken by the business in the area of data discovery.

Many organizations will find that they are only at the beginning of this effort and lack the required plan for GDPR. All companies must start with a basic framework. This will provide the foundation from which you will not only deliver compliance across the business but smooth the path to digital transformation in future. The right information governance program requires care-

ful identification of data types, data collection techniques, storage processes and further use cases, with documentation at each step of the way. The GDPR redefines user consent – users must agree to the way you intend to use and handle their data. So controllers and processors must be able to identify where data came from, whom it has been shared with and why. If you don't have a good handle on your data inventory, now is a perfect time to get started.

Next, the DPO needs to identify how the principles of the GDPR apply to the business. Companies at this stage will need to focus on identifying and managing the processes required under GDPR: conduct a risk assessment across the business, looking at how data is accessed, processed and stored, and align data with its associated risks so you can start implementing processes from data lakes to sovereign repositories. Where possible, enable technologies for automated controls over that data, so your business can become proactive. Data security should also be taken into account at this stage, with appropriate measures for incident response and special attention given to the period under which data must or can be stored, and where data should be pseudonymized (especially if your business uses data for test/dev requirements, business intelligence or other purposes).

Under an IG model, organizations can use a set of standards and requirements to identify, collect, store and secure information to meet business needs, comply with regulatory requirements or satisfy litigation (e.g., e-discovery) demands. By following common data security best practices, the organization will be better equipped to comply with not only GDPR, but with other regulations in future.

GDPR stipulates a number of areas that might trigger a need for process changes across the organization. These include mandatory data breach reporting (within 72 hours of an organization first becoming aware of the breach) and the right to erasure (also known as the 'right to be forgotten,' meaning a controller will have to stop disseminating data or have their service providers or third parties halt the processing of that data upon request).

Organizations must also implement measures to mitigate risk, and have these documented. Recording all policies and procedures set in action as a requirement of GDPR will be an ongoing obligation, and such policies and procedures will require constant review. Organizations should, therefore, set up processes for ongoing assessment of their GDPR compliance procedures and seek continuous improvement, especially as more details surrounding the regulation's specific requirements become clear.

Each organization will have their own roadmap for GDPR that will first identify the maturity of the organization in line with GDPR and other compliance requirements. Then, ideally, the roadmap will cover GDPR assessment, a GDPR program outline, data discovery activities, data access rights, data lifecycle activities, consent, and ways to manage individual rights and data protection, as well as breach management and other supporting services. Anonymization (so the data subject can't directly be identified) activities can also be included if required.

STEP 2: TOOL UP - SOFTWARE/SERVICES/SUPPORT

Once your organization has properly documented and adapted its privacy policy and put an IG roadmap in place, you can start to identify the tools, services and support required. The first consideration should be those services or tools that can help classify data, provide metadata or rules around ownership of that data, and ensure data integrity on its input, output, transmission and storage with the right validation checks in place. There are a range of tools to help with this. Remember, however, that while many software vendors promise to have the right solution for GDPR, the responsibility will ultimately rest with the controller or processor (i.e., you cannot offload your risk to a vendor).

There are many privacy impact assessment tools that can help assess your organization's data, and there are numerous e-discovery options that can help build out data-centric security policies around identified data types. Some of these have been used in the past for best practices following ISO models. Many will provide metadata tagging and can set rules for routines such as automated data retention, and increasingly these tools provide dashboards for GDPR health checks.

At this stage you need to consider not just structured data, but also unstructured data (key types of unstructured data include email attachments, web content, business documents, audio recordings and IoT data). Much of this unstructured data will not have been meta-tagged or identified properly in the past. This type of data can be used for business intelligence, and where possible may require anonymization, encryption or pseudonymization – or you might prefer to destroy some of this data altogether if it holds little or no business value. The key will be having metadata in good order – this will also help should you be asked to retrieve or migrate data upon customer request.

In future many companies will ultimately turn to artificial intelligence (AI) for better automation of some of these services, but for now, most companies start by doing a 'data stock-take,' combing CRM systems, creating master data management (a method to define and manage critical data) and even data lakes to ensure that data is stored in the right location, and in an easily accessible and reportable manner. Increasingly, organizations will consider using customer intelligence platforms that can consolidate a single view of the customer while adding a layer of data governance, synthesis and identity.

We have already seen data catalog software grow in importance with data rationalization and risk management software. In the case of unstructured data, a vast amount will also sit in unregulated file systems where access control is limited, and files are freely editable, so companies may also want to revisit their storage policies and look at technologies such as object storage, which creates a metadata record that follows the data element through its life, while allowing data management policies such as access rules, data protection, encryption and lifecycle management to be defined. At the same time, object storage can help overcome fears around future data growth, since this form of storage offers a scale-out architecture.

Other tools are available for line-of-business users to help provide the visualization of data flows, data storage and data types. For organizations working with a service provider, orchestration platforms could also be offered, allowing you to set your own levels of access and controls over data and where it resides with regional and global perspectives, as well as reports on who has accessed data and for what purpose. Many customer data platforms also have GDPR functions built in today that provide support for consent management, profile and access management, security and portability of data.

Information security and IG products are by no means the only way to manage risk for GDPR, but they can prove useful when identifying information assets, mitigating risk, ensuring privacy and combating fraud. IG is deployed in discrete technology offerings designed to accomplish prescribed tasks and also in enterprise-class software designed to meet a multitude of business objectives.

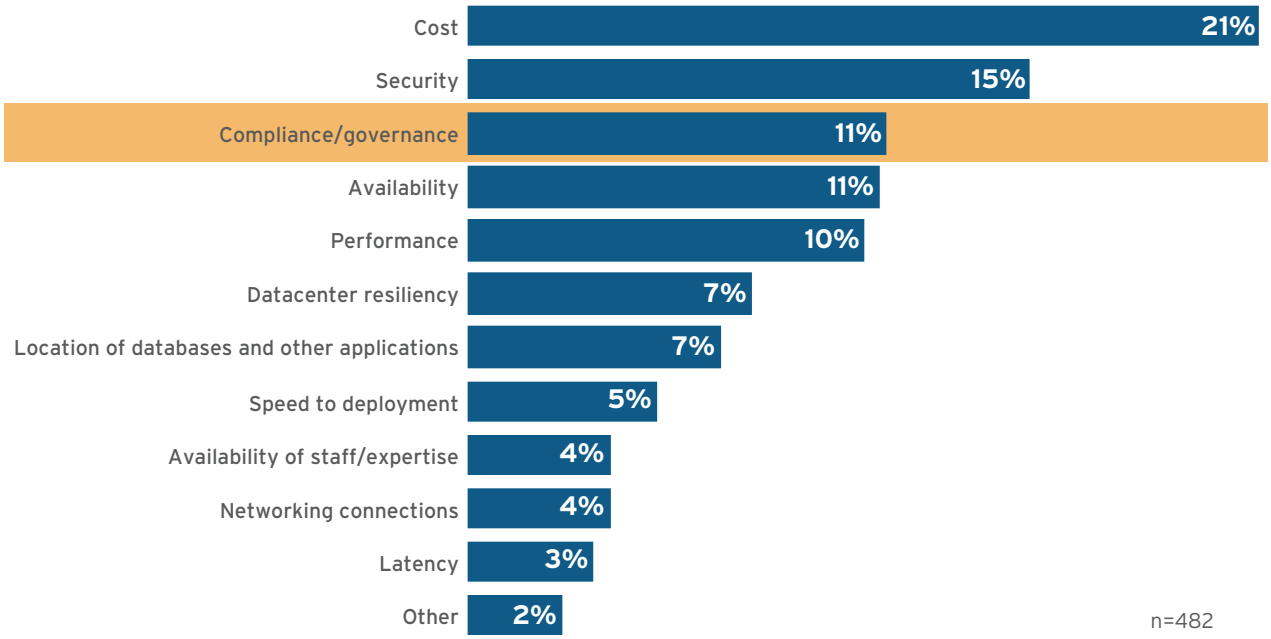
STEP 3: BEST EXECUTION VENUE AND DATA SOVEREIGNTY

Best execution venue (BEV) is a term borrowed from the financial services industry, where it refers to the ability to place orders and trade stocks or other financial instruments in the best possible environment to maximize return. In the context of cloud computing, BEV can be used to describe trends around automation and self-service, with the idea that specific applications or workloads are best processed or stored in a particular environment – an enterprise's on-premises server room, at a service provider, or in certain datacenters, for example – to provide the best efficiency, performance and cost profile.

Equally, BEV has led many enterprises (especially international organizations) to reconsider where their applications and workloads need to live from a geographic perspective, and this has driven many service and datacenter decisions. GDPR will place further emphasis on BEV as organizations look to identify the locations where workloads and applications must be processed in order to comply with data sovereignty regulations. Indeed, in a recent survey of enterprises (see Figure 3) conducted by 451 Research, compliance/governance factors were rated as the third most important criterion for determining the primary location of IT workloads, trailing only cost and security.

Figure 3: Influential Factors for Determining the Best Execution Venue for a Workload

(Respondents who own datacenters/server rooms or use colocation services)



Source: 451 Research, Voice of the Enterprise: Datacenter Transformation, Workloads and Key Projects 2018

Under GDPR, there are specific requirements for the transfer of 'personal data' across borders (the country in question must provide an adequate level of data protection, or this must be covered under contract law). And if the government of that country requires access to data pertaining to an EU citizen, this access must be agreed with the country and with the EU. For this reason, we have seen many enterprises move to establish implementation of services or establish a datacenter or server presence in the EU countries where they are operating. For the same reason, organizations should be aware of their telecom network choices to ensure that data in transit also stays within the boundaries the organization has set in its GDPR policy.

STEP 4: ROLE OF THE SERVICE PROVIDER/PARTNER - CHOICES AND BENEFITS

It should be evident by now that GDPR will present myriad challenges for many organizations. And there are myriad commercial options arising to help address some of these challenges – from legal experts to software vendors and specialist tools.

It is the service provider community, however, that is best placed to answer some of the questions organizations will inevitably have regarding GDPR. Many service providers are already controllers and processors of data, so they have had to examine GDPR compliance in detail for their own organization. Many also have internal legal teams and development teams that have been working on compliance-related technology solutions. Many also provide the services reach that might be required as organizations place some operations, for example, in specific European geographies.

The right service provider partner will be able to offer numerous options around data security and have strict policies in place for notification and monitoring of data breaches. We recommend asking your service provider about their data processing agreements (for each product/service you may be consuming, since these can differ with each) and the technical and organizational measures they have implemented to ensure adequate data protection. Many providers will offer templates for risk assessment under GDPR and will keep these updated as the regulation matures.

Most service providers and vendors today – even multi-tenant datacenter operators that do not process any data – have felt it their duty to help educate customers on GDPR. Many providers offer guidelines that, in some cases, come straight from national DPAs or industry organizations. In other cases, the providers themselves might be involved in producing DPA- and even EU-endorsed documentation. Find out where your service provider sits today and ask what they have planned regarding GDPR, and what support services for GDPR they have in place.

In time, some of the efforts being made by the service provider community, especially where guidelines are being issued, are likely to lead to new industry standards, so it is a good idea to keep abreast of the recommendations they provide.

Recommendations

- Organizations that have not done so already need to start creating a 'privacy by design' strategy around GDPR that allows the organization to identify the efforts required for compliance and to validate these efforts as they gain further understanding of the specific requirements of GDPR.
- Find out what skills you already have available within the company that can help build a GDPR compliance strategy, and seek a Data Protection Officer, either in-house or through an external organization.
- Begin by building up a level of understanding across your business regarding its operations, the data it uses, and how GDPR will apply to different parts of the organization and different data types.
- Actively plan for new technology and process implementations and ongoing risk assessments.
- Conduct a risk assessment across the business, examining how data is accessed, processed and stored, and align data with its associated risks so you can begin implementing processes from data lakes to sovereign repositories and enable technologies for automated controls over that data.
- Consider data sovereignty and best execution venue. Your data may need to live somewhere specific for performance reasons, but is it also best suited to a particular location for privacy and compliance reasons?
- Don't forget about data in transit – find out where your data travels to get from one destination to another, and if it remains GDPR-compliant during this journey.
- Don't be afraid to look outside of the organization for support – to data protection agencies, legal representatives, cloud and service providers, and systems integration firms. GDPR relies heavily on interpretation of the regulation, and many of your service provider partners will have already viewed GDPR through a number of lenses, helping to provide better insight.
- Be prepared to stay on top of your GDPR efforts. GDPR compliance will require constant assessment of the regulation and your environment in the coming years; the first cases that come before the courts could provide new insight and improve your understanding of the regulation.