REPORT

McAfee
Together is power.

Beyond the General Data Protection Regulation (GDPR):

Data residency insights from around the world

Table of Contents

3 Introduction

5 #1 Data in a Turbulent World

8 #2 Data Protection as Competitive Advantage

10 #3 GDPR: Awareness, Preparation and Response

14 **#4 Where is My Data?** Data storage, location and migration

16 **#5 Country-specific Regulations:** Understanding and impact

18 Summary

19 **Appendix:** Methodology and survey demographics

Introduction

As every business decision-maker should now know, the E.U. General Data Protection Regulation (GDPR) enforcement date is coming. The GDPR will be enforced starting May 2018 and will apply to those collecting, storing or using the personal data of the residents of the European Union's 28 member states. The Regulation changes requirements around protecting the personally identifiable information of over 500 million people, and occupies the minds of anyone around the world concerned with data protection.

The GDPR is not the only regulation affecting global business, of course, nor is it the only issue that concerns those charged with storing, processing, managing and protecting one of the world's most valuable assets: data.

To better understand data decision-making, McAfee® commissioned Vanson Bourne to survey the views of 800 senior business professionals across eight countries around the world from a range of industry sectors.

The following pages will shed light on how the respondent organizations currently approach data management, protection and residency (the physical location where data is stored). This report also explores the impact of global events such as:

- Geopolitical changes in several regions, and their impact on data
- The role of data protection as a competitive advantage
- The degree to which organizations are aware of, and prepared for, GDPR
- The driving factors behind data residency decisions
- The impact of 11 country- and sector-specific regulations

From the dozens of fascinating findings that follow, here are just nine:

1. Global events affect data migration plans

Nearly half of organizations plan to or say they will migrate data as a result of political changes, including GDPR, Brexit and changing policy approaches in the U.S. (See Section #1)

Organizations will spend $85,000 less on average in the United States because of U.S. government policies. (See Section #1)

McAfee™
Together is power.

2. **Privacy sells: Data protection delivers commercial advantage**

   Seventy-four percent of respondents believe organizations that properly apply data protection laws will attract new customers. (See Section #2)

3. **Public opinion is key to data decision-making**

   Eighty-three percent of organizations take public sentiment toward data privacy into account when making data residency decisions. (See Section #2)

4. **GDPR will make Europe the world's data leader**

   Seventy percent believe the implementation of GDPR makes Europe a world leader in data protection. (See Section #2)

5. **Organizations take 11 days on average to report a breach**

   GDPR requires that the local regulator is alerted within 72 hours of a data breach or be given reasons for the delay. Currently, it takes nearly four times as long – 11 days on average to report a breach. (See Section #3)

6. **Organizations expect cloud service providers to help with compliance**

   Eight in 10 organizations are planning, at least in part, to leverage their cloud service provider to help achieve data protection compliance. Some might be overestimating the degree to which cloud providers are accountable. (See Section #3)

7. **Most organizations are 'unsure' where their data is stored**

   Forty-seven percent of respondent organizations say they know where their data is stored at all times. That means the majority are unsure, at least some of the time. (See Section #4)

8. **The United States is the most popular data storage destination**

   Forty-eight percent of organizations in our survey expressed a preference for their data storage to be in the U.S., followed by Germany (35 percent), the U.K. (33 percent) and France (25 percent). (See Section #4)

9. **Only 2% of bosses say they know the full extent of the laws that apply to their organizations**

   The majority of respondents (54–74 percent) believe their organization has a "complete understanding" of the data protection regulations that apply to them. In fact, just 2 percent of senior decision-makers know all the clauses of regulations that apply to their organizations, a reflection perhaps of the complexity of those regulations. (See Section #5)

McAfee™
Together is power.

#1 Data in a Turbulent World

Rarely has the world experienced such flux. Economic and political upheaval is matched by accelerated digitalization, mass movement of populations and fears of physical and cyber terrorism. Laws regulating the use of personal data and those seeking to give governments greater surveillance powers in the name of national security do not operate in a vacuum. Rather, they operate in the context of this upheaval. They present a moral tug-of-war for policy-makers and the societies in which they operate, as well as a major dilemma for business organizations operating within them.

That's why the first part of this extensive report into the attitudes, actions and intentions of senior decision-makers explores the potential impact of geopolitical changes and a diverse set of events such as Apple's reluctance to grant backdoor iPhone access in the aftermath of the San Bernardino shootings of December 2015.

To what extent do globally recognized events influence data migration plans? According to the findings, nearly half of organizations will migrate data as a result of political changes, including the forthcoming E.U. General Data Protection Regulation (GDPR) (48 percent), the U.K.'s exit from the E.U. (48 percent), or U.S. policies (47 percent). Some are actively doing so today. Others have plans to do so.

Data Migration Plans

Is your organization actively migrating its data to a different location as a result of the following?

Event	Yes	No but plan to	No and no plan to	Don't know
GDPR	27%	21%	39%	13%
U.K. exit from E.U.	27%	21%	40%	12%
U.S. policies	27%	20%	40%	13%
Apple/San Bernardino	23%	18%	45%	15%
Microsoft/U.S. cloud access	25%	17%	44%	14%
Government surveillance	27%	17%	39%	17%

In response to three major events, 41 percent have or plan to migrate data as a result of the Apple/San Bernardino case; 42 percent in response to the Microsoft/U.S. cloud data access case; and 44 percent as a result of increased awareness around government surveillance. These are smaller numbers, but there remain substantial minorities who intend to act as a result of external events.

It's worth noting that migration does not necessarily mean moving data out of a relevant country. It might mean moving it into that country. For example, organizations may respond to the enforcement of GDPR in 2018 by storing data in one of the 28 E.U. member states (see Section #4 for more detail). On the other

"According to the findings, nearly half of organizations will migrate data as a result of political changes."

hand, organizations may choose to respond to the United Kingdom's exit from the European Union due in 2019 by moving data into or out of the U.K.—depending on customer location.

Those who work in the healthcare sector are more likely than others to respond to changes in the E.U. by rethinking their data migration plans. In both cases, 52 percent of respondents from the healthcare sector have already migrated data or are planning to do so.

Beyond migration plans, these world events are likely to have implications for technology acquisition and investment.

According to the senior decision-makers who responded, U.S. policies introduced by the current administration already have—or will have—an effect on technology acquisition investments in 63 percent of instances. The same number said E.U. realignment will impact technology investment while GDPR will have an effect in two thirds (66 percent) of cases.

These figures may reflect a belief shared by just over half of respondents (51 percent) that heavy-handed external data protection regulations are holding their organization back from adopting new technologies.

To get a sense of the level of investment decline, respondents were asked to quantify likely changes in spending over the next five years.

Average Change in Spend Over the Next Five Years

GDPR and spend within E.U.	-$83,654
U.S. policies and spend within U.S.	-$85,414

The findings suggest there will be a material reduction in spending as a result of geopolitical changes. The average reduction among all organizations as a result of government policies within the U.S. is projected to be $85,414 over the next five years. A similar reduction, $83,654, will result within the European Union because of GDPR. So while there may be a short-term increase in spending on GDPR compliance, overall enterprise spend might well decline. Perhaps as significant—and an illustration of ongoing uncertainty—a fifth of respondents do not yet know how U.S. policies (20 percent) and GDPR (19 percent) will impact enterprise spending.

Impact on Technology Investment

What do these results say about technology spend in the near to medium term? They suggest, at the very least, that a number of global events and a major forthcoming regulation are giving organizations pause for thought. Some will revise and review spending plans, while some may choose to reduce overall investment.

"The average reduction among all organizations as a result of government policies within the U.S. is projected to be $85,414 over the next five years."

These events are likely to have an impact on decisions around enterprise infrastructure and the ongoing role of cloud and cloud services. They may also lead to an increase in the number of data-focused recruits.

There are likely to be more urgent conversations about the geographic location of data on premise, in managed or dedicated data centers, in the cloud, or in a combination of all three. Data residency will rise up the corporate agenda, determining the questions asked of service providers and the location of managed infrastructure on a country-by-country basis.

This shouldn't be read, however, as a move away from cloud as an essential part of data provision. It may, however, encourage organizations to explore private rather than public infrastructure in the first instance.

McAfee
Together is power.

#2 Data Protection as Competitive Advantage

It's time to challenge conventional wisdom. Data protection is not only good practice, but a legal obligation to meet and an organizational requirement. It can offer an opportunity to get on top of data storage and locate every piece of data that resides within an organization, as well as a chance to reconnect with customers and clients, establishing consumer trust in the process.

The following findings bear out this progressive view of data protection.

Consider, for example, the fact that most organizations take public sentiment toward national data privacy into account when selecting where to store data. Accordingly, 47 percent of senior decision-makers in this survey said public mood influenced all their storage decisions, while a further 36 percent said it helped influence the decision. (See Section #4 for more on data residency).

Or how about the opportunities GDPR creates? Some challenging aspects of the E.U.'s forthcoming data protection regulation are discussed in the following section, but consider that seven in 10 senior business decision-makers believe Europe is leading the world in its approach to data protection. A similar number (67 percent) believe GDPR will help promote investment in Europe. In short, the protection of customer and other data through GDPR compliance could give some organizations a competitive advantage.

Some respondents consider data protection a competitive advantage and are able to measure its commercial impact. Nearly three quarters (73 percent) say they are able to quantify the value of security, including data protection, to the business while a similar number (74 percent) believe organizations are using data protection as a means of attracting new customers.

Rethinking the Value of Data Protection

Data protection may provide multiple business benefits. These benefits include the avoidance of fines and regulatory penalties, as well as the costs of dealing with the aftermath of a breach, for example. They may also include the retention of customer trust and the avoidance of reputational damage.

Meanwhile, compliance activities can have a benign effect on other business processes which, while not part of this study, are important.

With clean and secured data, a business can better trust the integrity of the analytics it is generating. To put it another way: no more "garbage in."

World Leaders?

70% of respondents agree with the statement, "Europe is a world leader in data protection by implementing the GDPR."

67% of respondents agree with the statement, "The GDPR will help promote investment in Europe."

Furthermore, lessons learned through compliance measures to protect customer information can be applied to other data, such as a company's intellectual property. No organization needs the value of its IP, nor the competitive advantage it affords, spelled out to them.

Finally, there is an impact on business culture that should not be underestimated, especially the effect it has on talent acquisition and retention. The protection of data is a proxy for a transparent and ethical approach to business, exactly the values today's workforce craves.

Competitive Advantage?

73% of respondents agree with the statement, "My organization is able to quantify the value of security to the business."

74% of respondents agree with the statement, "Organizations are using data protection to attract new customers."

#3 GDPR: Awareness, preparation and response

Business burden or entrepreneurial opportunity? The GDPR may be both.

Due to be enforced starting on 25 May 2018, GDPR is the successor to the 1995 Data Protection Directive. Although applicable to each E.U. member state, it is relevant to any company—regardless of country of origin—that collects, stores and uses the data of E.U. residents as either customers or employees. It is relevant to any organization that has staff but no clients or customers in Europe.

GDPR is long-awaited because much has changed since 1995. Two decades ago, the commercial internet was in its infancy and most of the data an organization held was stored within its perimeter, typically on premise. While some corporate functions were out-sourced, and data was transferred for payroll, for example, the number of third-party vendors and the complexity of their tasks has changed dramatically. Today, data access is 24/7, on demand, mobile and cloud-based. Meanwhile, the Internet of Things, machine learning and artificial intelligence have changed our understanding of what constitutes personally identifiable information (PII), its access and its use.

GDPR is not only the most ambitious piece of data protection regulation this century—directly affecting a trading bloc with a combined population of over 500 million people—it is perhaps the most complex piece of data-related legislation anywhere in the world, raising the bar for all those operating in Europe, bringing it in line with the most stringent protection regulations that currently apply in the Netherlands and Germany. It also brings together security and privacy in a way that hasn't been done before and continues to allow member states to make local variations.

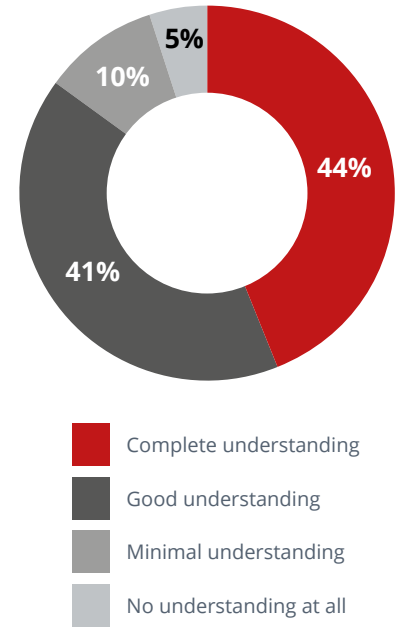
In terms of those who need to be ready for May 2018, 86 percent of respondents believe their organization has either a "good" or "complete understanding" of GDPR.

Of those respondents who have minimal or no understanding of what GDPR means to them, there is notable variation by sector and size of company. For example, 27 percent of public sector organizations say they have minimal or no understanding while that is the case for only 8 percent of private healthcare companies. Meanwhile, organizations of 5,000 employees or more rated themselves lowest by this measure, with 19 percent of respondents suggesting minimal or no organizational understanding of GDPR. This high figure may reflect the difficulty larger organizations face.

Notwithstanding this, the generally high level of understanding might reflect the time organizations claim they have spent planning for GDPR—24 months on average, with just under half (47 percent) planning for more than two years.

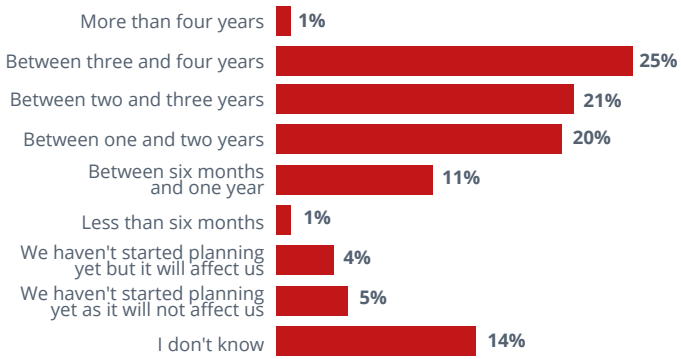
Understanding GDPR

Those respondents whose organization does business within the E.U. were asked, "To what extent does your organization understand what the GDPR means to them?"



Planning for GDPR

How long has your organization been planning for the upcoming E.U. data protection regulation (the GDPR)?

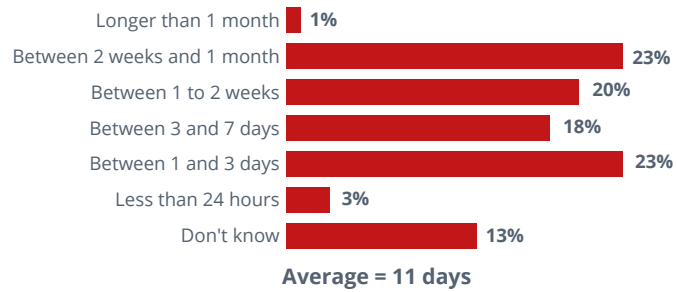


To illustrate the pervasive nature of European-related legislation, consider that three quarters of survey respondents, regardless of country of origin, currently do business within the E.U., with a further 13 percent not conducting business there but planning to. Only one in 10 organizations insists it has no plans to do business in Europe, a figure skewed by the 21 percent of public sector organizations that answered no. It's worth repeating that any organization that collects, stores or uses the PII data of European Union residents will fall under the auspices of the GDPR, regardless of whether they consider themselves actively carrying out business in the E.U. or whether they ever let the data leave the E.U.

Among the significant new elements of GDPR, especially for companies focused in the E.U. where not all countries have laws around data breach reporting, is the requirement to report a breach to the regulator "without undue delay, and where feasible, not later than 72 hours" of becoming aware of it or explain the reasons for the delay. Are organizations in a position to do this? The findings suggest it will be a challenge. Asked how quickly they thought they could report a breach today, only a quarter (26 percent) believe they could meet the three-day deadline.

Readiness to Report Breaches

On average how quickly can your organization report a breach of your defenses in regards to personal data that you hold?



On average, it takes organizations 11 days to report a breach of their defenses, nearly four times longer than necessary to meet GDPR's timetable. Nearly a quarter of respondents say it takes two weeks or more. On a more positive note, 78 percent of respondents are either set up to report a breach to a third party or are planning to be able to do so.

"In terms of those who need to be ready for May 2018, 86 percent of respondents believe their organization has either a "good" or "complete understanding" of GDPR."

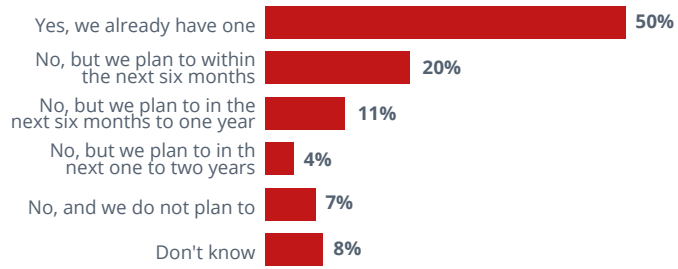
Digging a little further into attitudes toward breach notices, the findings suggest that the majority of organizations believe there's a stigma associated with reporting a data violation and nearly half (47 percent) would prefer to accept a fine rather than make a breach public.

When asked to explore the negative impact of a data breach, organizations identified loss of customer confidence (58 percent), loss of customers (46 percent) and financial penalties (45 percent) as the three worst outcomes. And when asked how they would cover the cost of a breach incident, 44 percent said they would look to pay for it—at least partially—through an insurance policy, while 39 percent said they would draw on an allocated budget.

GDPR also requires that most organizations employ a data protection officer (DPO). The vast majority of organizations (81 percent) surveyed for this research already have one in place or will have one in place before GDPR takes effect—it's already a requirement for certain companies in certain E.U. member states. However, the research suggests that for two thirds of organizations GDPR is either the "only" or the "main" reason for employing a DPO.

Employing a Data Protection Officer

Has your organization employed a data protection officer?



Finally, respondents were asked if their organization plans to take advantage of its cloud service provider (CSP) to help it achieve data protection compliance. A large majority (80 percent) said they do plan to, with 38 percent intending to pass data controller responsibility to their CSP, which is not allowed by the regulation. The remaining 42 percent accepted that, as codified in the GDPR, despite reliance on the cloud service provider, significant responsibility is likely to remain with the organization itself.

Reliance on Cloud Service Providers

Does your organization plan to leverage its cloud service providers to help you achieve data protection compliance?	
Yes, definitely, we have/will pass data controller responsibility to them	38%
Yes, to an extent, although responsibility will remain with us	42%
No, they will never be responsible for managing the personal data we hold	12%
Don't know	8%

Attitude toward reporting breaches

63% agree that, "In my industry, reporting a breach has a stigma attached to it that will have a negative effect on our brand."

47% "would rather risk a fine than admit a breach because of the negative impact a declaration of a breach would have on the brand."

Yet when asked if they agree that "organizations are incorrectly placing their faith in cloud service providers to manage GDPR for them," 58 percent said yes. The advice for those organizations engaging cloud service providers is simple: read the small print. Why? Because uncertainty remains until enforcement begins. GDPR introduces explicit responsibility on the processor for the first time. However, that may not mean that ultimate responsibility shifts substantially to a cloud service provider.

Controllers and Processors

To quote the GDPR, "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." And while processors such as cloud service providers do have obligations under GDPR, it is for the controller to ensure they employ only processors—including CSPs—"providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation."

"GDPR also requires that most organizations employ a data protection officer (DPO). The vast majority of organizations (81 percent) surveyed for this research already have one in place or will have one in place before GDPR takes effect."

#4 Where is My Data?

Data storage, location and migration

As this report makes plain, the residency of data has become a strategic decision for most organizations, accelerated by four interrelated factors. First, factors such as geopolitical change are influencing data location. Second, there is also impact from a changing regulatory framework – that means varied and, in some cases, tightening data protection regulations coupled with governmental attempts to gain greater access to mass communications data. Third, the nature of data storage and transmission has changed dramatically over the last two decades, notably as a result of the growth of the commercial internet and cloud computing as a model of choice. Finally, there is the increasing commercial value of data in the digital era.

As a result, the need to answer a seemingly simple question—where is my data?—has risen up the organizational agenda.

An overwhelming 97 percent of respondents are confident that they have some knowledge of where their data is physically stored. Dig a little deeper, however, and a smaller 47 percent say they know where their data is stored at all times. Of the remainder, 41 percent know the country it is stored in most of the time, while 9 percent know the world region but not the specific country. While specifics may not matter in some instances, it will in others. For example, it may be become essential to know that data is stored in the U.K. rather than simply somewhere in Europe.

Asked why they chose a particular location for data storage, 46 percent of respondents indicated that they were led by data protection regulation in that country.

Reasons for Storage Location

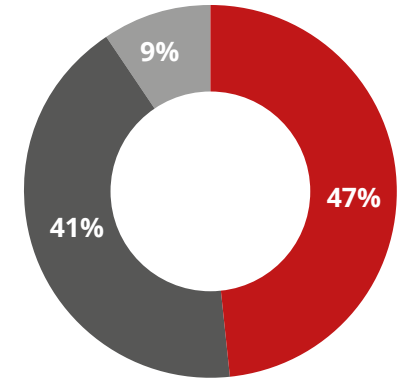
Why does your organization store its data in the country that it does?	
Data protection regulation laws in that country	46%
My organization requires us to store data in that country	37%
Our chosen cloud service provider is located in a specific location (the CSP is more important to us than the location)	34%
Cheaper provider costs	30%
Reputation of security	30%
Vendor lock-in	23%

Among other responses, a third (34 percent) said location is led by their cloud service provider of choice, 30 percent cited cost and reputation of security, while nearly a quarter (23 percent) said that their hands were tied by their technology vendor.

It is not just protective legislation that influences storage decisions—laws such as the U.K.'s Regulation of Investigatory Powers Act (RIPA) and the U.S. Patriot Act, designed to grant government bodies greater access to surveillance data, also play a part in organizational decision-making.

Where is my data?

How confident are you that you know where your organization's corporate data is physically stored?



Completely confident – we know where all of our data is all of the time

Somewhat confident – we know the country it is stored physically in most of the time

Somewhat confident – we know the region it is stored physically in all of the time, but not the specific country it is physically in

Six in 10 (61 percent) respondents admit that laws negatively affect where their organization's data is stored. Over three in 10 say that RIPA (32 percent) or the Patriot Act (31 percent) stop organizations storing data in the U.K. and the U.S., respectively. A larger proportion (35 percent) suggest that GDPR will deter them from storing data in relevant European Union countries. Just under a quarter (23 percent) insist that there are no laws that deter their organization from storing data in any country.

Storage Deterrence

What laws deter your organization from storing its data in the country where they are relevant?	
GDPR	35%
RIPA	32%
Patriot Act	31%
No laws	23%

Regardless of laws that might act as a deterrent, the U.S. (48 percent) is the single most popular country to store data in, followed by Germany (35 percent) and the U.K. (33 percent).

These preferences largely reflect where organizations currently store their data. Today, the top three locations are the U.S. (41 percent), the U.K. (25 percent) and Germany (22 percent). They also reflect the nations that most believe have the toughest data protection requirements. The U.S. (68 percent) is top of the list again, followed by the U.K., Germany and France. Intriguingly, those resident in each country believe their native land has the most stringent rules: 96 percent of Germany-, 89 percent of U.S.-, 88 percent of U.K.- and 79 percent of France-based decision-makers. (For more on some of the main regulations affecting each of the countries in this research, see section #5 below.)

Tough Laws

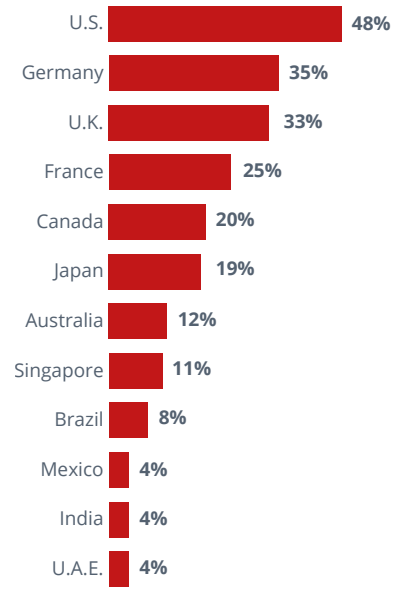
Which three countries do you believe have the most stringent data protection requirements (e.g., laws, policies, procedures, etc.)	
U.S.	68%
U.K.	57%
Germany	53%
France	35%

By contrast, when asked which country to avoid when considering storage decisions, the list is topped by Mexico (38 percent), India (28 percent), Brazil and South Africa (both 27 percent).

The popularity or otherwise of countries as data storage destinations is likely to reflect perceptions of the different data protection regimes in different parts of the world. The impact of those country-specific regulations is explored in the next section.

Storage Preference

Which countries would you prefer to store your organization's data in because of the data regulation requirements within those countries?



#5 Country-specific Regulations:
Understanding and impact

Any organization with global ambitions, workforce and customers will soon butt up against myriad country-specific regulations. Throw in sector-specific laws—designed, for example, to protect banking customers or hospital patients—and myriad becomes matrix.

As discussed earlier, GDPR (see Section #3) will bring consistency to data protection laws within the E.U.'s trading bloc of over 500 million consumers, but elsewhere there's nothing but complexity. Consider, for example, that some countries don't have a single, omnibus piece of legislation devoted to the protection of personal data. Rather, the U.S. invokes a multitude of sector-specific laws to define and enforce the scope of data use. Equally, there are countries that partially devolve data protection to federated states: Germany and (again) the U.S.

It is in this context that the McAfee/Vanson Bourne survey results shed light on the understanding of, comfort in adhering to and deep knowledge of 11 relevant data protection regulations that take us from Australia, Japan and Singapore in the Asia-Pacific region to the United States via France, Germany and the U.K. in Europe.

Where relevant, the majority (52–74 percent) of respondents say that their organization has complete understanding of the regulations covered in Australia, Germany, the U.K. and the U.S. The exception is GDPR (44 percent), a regulation yet to be enforced. Elsewhere, only a minority claim complete understanding of regulations in Brazil (40 percent), Singapore (34 percent), France (28 percent) and Japan (13 percent).

Understanding tends to correlate with comfort in adhering to a particular regulation. However, the levels of comfort tend to be far lower than both claimed knowledge and understanding. In only two cases—the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Federal Trade Commission Act—are more than half of respondents "extremely comfortable" with adherence.

Tough Laws

Asked "How comfortable is your organization with adhering to the following data protection regulations?," the following percentage said they were "extremely comfortable":

HIPAA (U.S. Healthcare)	54%
FTC Act (U.S.)	50%
Financial Services Modernisation Act (U.S.)	42%
Privacy Act (Australia)	42%
BDSG (Germany)	38%
DPA (U.K.)	34%
Brazilian Civil Rights Framework for the Internet	32%
GDPR (Europe)	30%

"Where relevant, the majority (52–74 percent) of respondents say that their organization has complete understanding of the regulations covered in Australia, Germany, the U.K. and the U.S."

Tough Laws

Asked "How comfortable is your organization with adhering to the following data protection regulations?," the following percentage said they were "extremely comfortable":	
PDPA (Singapore)	20%
DPA (France)	18%
APPI (Japan)	10%

Respondents were then asked to identify specific clauses within relevant regulations. Rather than express their sense of readiness, this question explored the detail of their knowledge. It threw up some interesting findings. For example, just 2 percent of senior decision-makers knew all clauses of the data protection regulations relevant to them.

Senior Decision-Makers' Understanding of the Laws

Analysis of the average percentage of clauses respondents correctly identified as related to the following data protection regulations:	
BDSG (Germany)	55%
DPA (U.K.)	52%
GDPR (Europe)	51%
PDPA (Singapore)	49%
Privacy Act (Australia)	49%
Brazilian Civil Rights Framework for the Internet	48%
HIPAA (U.S. Healthcare)	47%
FTC Act (U.S.)	42%
APPI (Japan)	41%
DPA (France)	39%
Financial Services Modernisation Act (U.S.)	38%

On average, German respondents could identify 55 percent of the clauses that relate to Bundesdatenschutzgesetz, the country's federal data protection act. That proved to be the highest average across all 11 regulations. Most identified fewer than half of relevant clauses.

Perceived comfort and understanding don't necessarily add up to deep knowledge. For example, 74 percent of relevant respondents expressed "complete understanding" of HIPAA, yet on average they were only able to identify 47 percent of the Act's clauses. Similarly, three quarters of those that need to comply with the Financial Services Moderation Act said they had complete understanding, yet they knew only 38 percent of the Act's specific regulations.

By contrast, some of those expressing little confidence in their knowledge—those expected to adhere to Singapore's Personal Data Protection Act or the E.U.'s GDPR, for example—turned out to know more than their contemporaries.

While not every decision-maker needs intimate knowledge of every clause of every relevant regulation, the business does need that knowledge. These results suggest more education is required, which in turn may help organizations adhere to the regulations.

Summary

There is much to consider from the findings discussed over the previous five chapters. This report provides a context in which to compare individual and organizational attitudes toward data residency, protection and preparedness in the light of a changing regulatory landscape. It also provides a comprehensive view of how senior decision-makers view 11 key data regulations from around the world, including the forthcoming GDPR.

One of the most notable themes that runs through the findings is an apparent contradiction in the impulses of respondents. On the one hand, global events and a tightening data protection regime is giving senior decision-makers pause for thought over organizational spend and investment. On the other hand, most organizations looking for the best place to locate their data gravitate toward those countries with the most stringent data protection rules.

So while compliance might be burdensome and disruptive in the short term, there is a recognition—albeit tacit—that firmer data protection rules are beneficial not just to customers and clients but to the organization itself. This is perhaps best articulated in the belief that data protection can be turned into a competitive advantage, a so far under-explored boon.

Through the uncertainty there is much to be positive about. Good data governance underscores good organizational management. Organizations will make better use of their data the more they understand what they possess and where it resides. As this report makes plain, there is much to learn.

To find out more about the data protection opportunity for businesses, visit McAfee's GDPR site: **mcafee.com/GDPR**.

"Firmer data protection rules are beneficial not just to customers and clients but to the organization itself."

Appendix: Methodology and Survey Demographics

Research into "Data Protection Regulation" was conducted by Vanson Bourne on behalf of McAfee with field work running from April to May 2017. The findings are based on the responses of 800 senior business decision-makers from across eight countries and a range of industry sectors and sizes, starting at those with 500 employees.

Interviewees by Country:

Australia:	100
Brazil:	50
France:	100
Germany:	100
Japan:	100
Singapore:	50
United Kingdom:	100
United States:	200

Interviewees by Function:

Information technology	26%
Finance	11%
Business direction and strategy	10%
Health and safety	10%
Business development/sales/channel	9%
HR/training	6%
Client services/relationship management	5%
Operations	4%
Engineering	3%
Design/research and development	3%
Marketing communications	3%
Trading/merchandising/retail shop floor	2%
Quality control	2%
Risk/fraud/compliance/governance	2%
Legal	2%
Purchasing/procurement	1%
Facilities/property	1%
Production/manufacturing	1%
Logistics/supply chain/transport/fleet	1%

Interviewees by Industry Sector:

Financial services:	200
Private healthcare:	200
Public sector:	200
Other enterprise sectors:	200

Interviewees by Organization Size:

500-999 employees:	201
1,000-2,999 employees:	215
3,000-4,999 employees:	204
5,000 or more employees:	180

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

*Methodology
The research, carried out by Vanson Bourne, interviewed 625 IT decision makers with influence over their organization's security solutions. Respondents were from private and public organizations with a minimum of 500 employees, with particular focus on the critical infrastructure sectors of finance (159 respondents), energy (139 respondents), transport (130 respondents), and government (128 respondents). The research was undertaken in the US, UK, France, and Germany. There were 250 interviews conducted in the US and 125 in each of the other countries.

The full data set is available on request

1. www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml
2. McAfee Labs Threats Report, May 2015, www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf
3. www.mcafee.com/us/resources/reports/rp-dissecting-top-5-network-methods-thiefs-perspective.pdf www.aspeninstitute.org/video/future-cyber-threats-featuring-lisa-monaco
4. https://communities.intel.com/docs/DOC-1151

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com