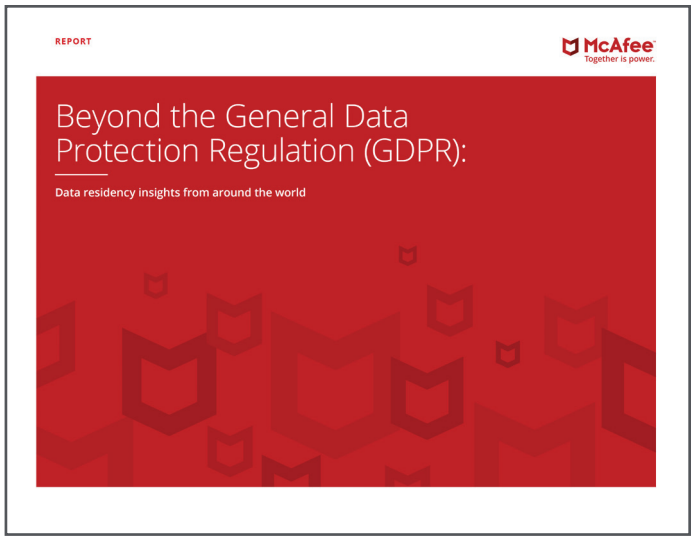
McAfee
Together is power.

Beyond the General Data Protection Regulation (GDPR)

Data residency insights in financial services from around the world



Learn More

To read the full report, please visit us at **www.mcafee.com/beyondGDPR**

The E.U. General Data Protection Regulation (GDPR) will be enforced starting May 2018, with new requirements applying to those collecting, storing, or using personal data of E.U. citizens.

The residency of data has become a strategic decision for organizations in the financial services sector, accelerated by several interrelated factors. These include geopolitical change, the impact of a changing regulatory framework around the world, the changing nature of data storage and transmission, the growth in cloud computing (such as recent recommendations released by the European Banking Authority), and the increasing commercial value of data in the digital era.

"The uncertainty of global events and the burden of greater regulation will have a negative impact on investment over the next five years."

Connect With Us

This survey into data protection regulation explores the impact of geopolitical changes and their impact on data, the degree to which organizations are prepared for the GDPR, and the impact of 11 country and sector-specific regulations. Conducted by researcher Vanson Bourne on behalf of McAfee in 2017, it includes the responses of 800 senior business professionals across eight countries and a range of industry sectors.

This executive summary examines the survey responses from the 200 respondents in the financial services sector to better understand the factors driving their data decision-making and how they currently approach data management, protection, and residency.

Key Findings

- **Global events impact financial services tech investment and data residency decisions**

  Major geopolitical events and forthcoming regulations are already having an impact on investment decisions by financial services organizations. Respondents said the GDPR (30%), the U.K.'s withdrawal from the E.U. (29%), and U.S. policies (29%), have already had an impact on technology acquisition investments. Those three events will continue to have an impact on those investment decisions in the future, along with government surveillance.

  Looking at the spending plans of financial services firms, the survey shows that, as with other industry sectors, the U.K.'s withdrawal from the E.U. and U.S. policies will have a negative impact. However, financial services differs from other industry sectors when it comes to spending within the E.U. due to the impact of the GDPR, with investment predicted to increase rather than fall. The overall change in investment by financial services firms as a result of these events breaks down as:

  - Investment within the U.K. down by $243,343 on average in the next five years due to the U.K. leaving the E.U.
  - Investment within the U.S. down by $25,739 on average in the next five years due to U.S. policies
  - Investment within the E.U. up by $64,649 on average in the next five years due to the GDPR

Will any of the following movements have an impact on your organization's technology acquisition investments?

Base: respondents from organizations in the financial services sector

Event	Yes, it already has	Yes, it will	No impact	I don't know
U.K. exit from the E.U.	29%	43%	20%	8%
GDPR	30%	42%	20%	10%
U.S. policies	28%	35%	27%	11%
Apple/San Bernardino	19%	30%	37%	15%
Microsoft/U.S. cloud access	21%	38%	29%	12%
Government surveillance	24%	36%	26%	14%

These global events are also affecting data migration, with just under half of financial services respondents saying their organization is either already actively migrating its data to a different location or plans to because of the U.K. withdrawal from the E.U. (48%), the GDPR (46%), or U.S. policies (44%).

"While financial services organizations find tougher data protection regulation burdensome, they also prefer to store data in those countries with the toughest laws."

- **Tough laws and public sentiment guide location for financial services data storage**

  The three countries financial services organizations would most prefer to store their data are the U.S. (49%), the U.K. (44%), and Germany (38%). This corresponds with the countries that financial services firms surveyed believe to have the most stringent data protection laws. It suggests that while financial services organizations find tough data protection regulation burdensome, they also prefer to store data in those countries with the toughest laws. In fact, almost half (48%) of financial services respondents cited data protection regulations as the top reason behind the choice of location for storing data.

  Some 45% of financial services organizations also say they consider public sentiment about a country's national data protection laws, to an extent, when considering the choice of physical location to store data. This is a higher percentage than in the full survey responses where 39% said that public sentiment is a factor with these choices. This indicates that concern about how data protection perceptions could impact their reputation and/or brand is of high importance to financial services companies.

  There are, however, a range of factors guiding the choice of where to store data that mean organizations are unable to always consider public sentiment in all of their data protection choices. According to the survey responses, the main factors include organization requirements (37%), location of their cloud service provider (CSP) (35%), or being locked in to a particular vendor (27%).

- **Customer confidence and financial penalties have biggest negative data breach impact**

  Financial services firms are better equipped for reporting a data breach than any other industry sector in the survey, taking nine days on average compared to between 10 and 12 days for the other sectors. More than a quarter (27%) are also set up to report in three days or less, which is already in compliance with the 72-hour breach reporting period for the GDPR.

  Loss of customer confidence is cited as the biggest negative impact of most concern to financial services organizations (64%), followed by loss of customers (51%), and financial penalties (48%).

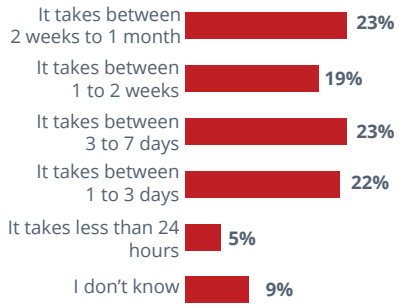
  Nearly three-quarters (73%) of financial services firms agree or strongly agree that there is a stigma in reporting a breach because of the negative effect on brand, and more than half (54%) say they agree or strongly agree that they would rather risk a fine than report a breach because of this.

- **Understanding of financial services data protection regulations is high but more education needed on the GDPR**

  The regulations that most apply to financial services organizations when it comes to data protection are the GDPR (82%), the U.S. Financial Services Modernization Act (25%), and the U.S. Federal Trade Commission (FTC) Act (25%). There are high levels of stated 'complete' understanding reported by financial services firms for these regulations, particularly for the FTC Act (76%) and U.S. FSMA (74%). Financial

Data breach reporting times

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



Average = 9 days

services respondents also reported high levels of understanding for the U.K. Data Protection Act (72%) and Germany's Bundesdatenschutzgesetz (BDSG) (72%).

However, only 44% of financial services respondents said they had a 'complete' understanding of the GDPR even though, on average, financial services firms have been planning for the GDPR for two years. A higher proportion (28%) of financial services organizations than other industry sectors have been preparing for longer, in the three-to-four-year timeframe.

The survey also highlights the lack of understanding among senior employees of the data protection laws relevant to their organization and industry sector. Senior professionals were able to correctly identify only 38% of clauses as relating to the financial services-specific FSMA and just 52% of the GDPR clauses. This suggests there is an education requirement to help employees better understand these data protection regulations to help their organizations comply.

Conclusions

This report provides valuable insight into individual and organizational attitudes in the financial services sector toward data residency, data protection, and preparedness for the changing regulatory landscape.

One of the 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 are giving senior decision-makers pause for thought over organizational spend and technology investment–although, unlike other sectors, the GDPR looks set to lead to an increase in investment by financial services organizations over the next five years. On the other hand, most of the financial services organizations surveyed gravitate toward those countries they believe to have the most stringent data protection rules–the U.S., the U.K., and Germany–when looking for the best place to locate their data.

While compliance might be burdensome and disruptive in the short term, there is some recognition that firmer data protection rules are beneficial not just to customers and clients but to the organization itself. They offer the opportunity to get on top of data storage and locate every piece of data that resides within an organization. Moreover, there is the progressive view, particularly in financial services, that data protection can be turned into a competitive advantage. Some 80% of financial services respondents believe organizations that properly apply data protection laws will attract new customers.

"Some 80% of financial services respondents believe organizations that properly apply data protection laws will attract new customers."

Clearly, benefits also include the avoidance of fines, reputational damage, and regulatory penalties.

Through the uncertainty of global events and forthcoming regulations, there is still much to be positive about. But there is still room for improvement in the time it takes to respond to breaches. And there is the need for more education throughout organizations with much still to learn about what data they possess, where it resides, and what regulations apply.

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

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.

Learn More

To find out more about the data protection opportunity for businesses, visit **www.mcafee.com/beyondGDPR**

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com