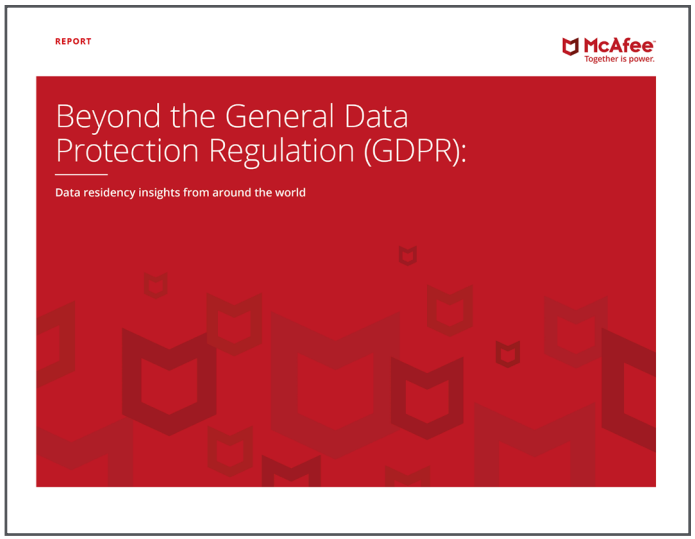
McAfee
Together is power.

Beyond the General Data Protection Regulation (GDPR)

Data residency insights in private healthcare 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 healthcare 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, and the increasing commercial value of data in the digital era. Health data is also a special category of data under the GDPR, as it has been under the E.U. Data Protection Directive.

"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 private healthcare 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 healthcare technology investment and data residency decisions**

  Major events on the world stage are already having an impact on the investment decisions of private healthcare organizations. Around a third of senior business professionals from the private healthcare sector said U.S. policies (34%), the GDPR (32%), and the U.K.'s exit from the E.U. (29%) have already had an impact on their organization's technology acquisition investments and will continue to in the future. Notably, the impact of government surveillance looks set to rise up the agenda and have a greater impact on technology investment in the future.

  Digging deeper into the spending plans of private healthcare services firms, the survey found that the uncertainty of global events and the burden of greater regulation will have a negative impact on investment over the next five years. That impact breaks down as:

  - Investment within the U.K. down by $208,993 on average in the next five years due to the U.K. leaving the E.U.
  - Investment within the U.S. down by $107,226 on average in the next five years due to U.S. policies
  - Investment within the E.U. down by $73,765 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 private healthcare sector

Event	Yes, it already has	Yes, it will	No impact	I don't know
U.K. exit from the E.U.	29%	39%	23%	10%
GDPR	32%	38%	17%	14%
U.S. policies	34%	35%	20%	12%
Apple/San Bernardino	19%	27%	36%	19%
Microsoft/U.S. cloud access	22%	32%	30%	17%
Government surveillance	24%	40%	23%	14%

"Just over half (53%) agree or strongly agree that they would rather risk a fine than report a breach."

World issues are also affecting data migration plans, with over half of private healthcare organizations saying they are already actively migrating their data to a different location or plan to because of the U.K. withdrawal from the E.U. (52%), the GDPR (52%), or U.S. policies (49%).

- **Tough laws and public sentiment guide location for private healthcare data storage**

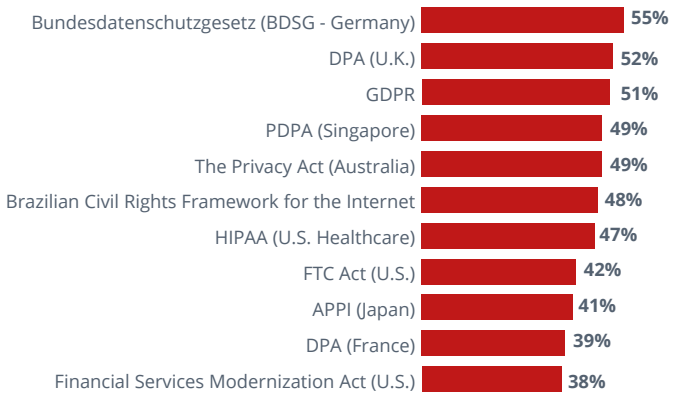
The U.S. has by far and away the most stringent data protection regulations, according to 74% of respondents in the private healthcare sector. That response is most likely based on the Health Insurance Portability and Accountability Act (HIPAA) regulation passed by Congress in 1996. The second most stringent data protection regulations are in Germany (57%) and then the U.K. (52%).

Yet those same countries are the ones most private healthcare organizations say they would prefer to locate their data–the U.S. (54%), Germany (38%), the U.K. (30%). And only 9% say they would avoid storing data in the U.S. because of its data protection regulations. This also aligns with where most of the responding private healthcare organizations store their data currently.

More than half (53%) of private healthcare respondents also take public sentiment about a country's data protection regulations into consideration, to some extent, when choosing where to store data, with a third (33%) considering it a factor in all of their data protection choices. The survey suggests there is a range of factors guiding the choice of where to store data that means organizations are unable to always consider public sentiment in all of their data protection choices. These factors include organizational requirements, location of their cloud service provider (CSP), or being locked in to a particular vendor.

Understanding of global data protection regulations

Average percentage of clauses respondents correctly identified as relating to the listed data protection regulations



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

Loss of customer confidence is cited by more than half (58%) of private healthcare respondents as the biggest negative impact they are most concerned about if their organization suffered a data breach, followed by financial penalties (50%), and loss of customers (48%).

"There is an education requirement to help employees better understand these data protection regulations."

Private healthcare organizations appear slightly better equipped for reporting a data breach than most other sectors, taking 10 days on average, compared to 11 days across all sectors. However, only just over one in five (21%) is set up to report a breach in three days or less, which is the timeframe for compliance with the 72-hour reporting period for the GDPR.

More than half (59%) of private healthcare firms agree or strongly agree that there is a stigma in reporting a breach because of the negative effect on brand and just over half (53%) agree or strongly agree that they would rather risk a fine than report a breach because of this.

- **General data protection awareness is good but more education needed on the GDPR**

The main data protection regulations that apply to private healthcare organizations are the GDPR in the E.U. (75%), HIPAA in the U.S. (25%), and the Federal Trade Commission (FTC) Act (25%), also in the U.S.

Not surprisingly, general understanding of the healthcare-specific HIPAA appears to be strong in the private healthcare sector with almost three-quarters (74%) of respondents saying they have complete understanding of the Act. The remaining 26% say they have a good understanding of the Act. There is also a high level of understanding of the FTC Act, where 70% say they have a complete understanding and 18% have a good understanding.

However, complete understanding of the GDPR among private healthcare respondents is significantly lower (46%). But almost half (47%) say they have a good understanding of the GDPR. Private healthcare firms have, on average, been planning for the GDPR for two years and a significant proportion (48%) have been planning for a longer timeframe of two to four years.

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 fewer than half (47%) of clauses as relating to the healthcare-specific HIPAA 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 private healthcare 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. On the other hand, most organizations looking for the best place to locate their

"Nearly three-quarters (73%) of private healthcare respondents believe organizations that properly apply data protection laws will attract new customers."

data gravitate toward those countries they believe to have the most stringent data protection rules–the U.S., the U.K., and Germany.

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 that data protection can be turned into a competitive advantage. Nearly three-quarters (73%) of private healthcare 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