VansonBourne

EU General Data Protection Regulation (GDPR)

Are you ready for it?

ca technologies

Contents

Foreword and Introduction

Foreword

The General Data Protection Regulation (GDPR) is a new piece of European Union (EU) legislation that has taken years of negotiation. It is widely regarded as the biggest change to the digital privacy landscape in Europe for over 20 years – and in today's growing digital economy, having clear laws with policies in place is more important than ever before.

In June 2016, the UK held a referendum, which resulted in a vote to leave the EU. What do the results of the referendum mean for UK organizations? Do they still need to comply with the GDPR?

As the US-based respondents in this study recognise, any organization outside of the EU that wants to trade within the European Single Market will need to comply with the GDPR by May 25th 2018, regardless of their country's membership of the EU.

Despite this understanding, this paper shows that there is a lot of work to be done on both sides of the Atlantic to ensure GDPR compliance. The GDPR has expanded the definition of personal data and this will put IT and testing departments on high alert to safeguard personal data, across both testing and development environments.

Organizations will need help, and CA Technologies offers a range of solutions that can assist organizations in their program's to comply with the GDPR, thereby helping your business compete in today's globalized, digital world.

Christoph Luykx

Director, Government Relations EMEA

CA Technologies

Introduction

In this paper, you will find the results of a survey commissioned by CA Technologies to understand the readiness of organizations to meet the compliance needs of the GDPR. Given the GDPR is set to have wide-ranging implications for the type of data that can be used in non-production environments, CA Technologies wanted in particular to understand how companies are planning for the GDPR and what processes and technology is needed to help them.

Scope of the research

This paper is based on the findings from a research survey undertaken by Vanson Bourne. Interviewing started the week that the GDPR was announced (April 2016). A total of 200 B2B interviews were conducted; 167 IT decision makers (ITDMs) and 33 risk and compliance decision makers (RCDMs). 98/200 respondents are C-suite level individuals, the remainder are senior managers.

The respondents are from organizations with at least 500 employees, and a global annual revenue of over $1 billion and from a range of sectors, including:

- Financial services (including insurance)
- Manufacturing
- Retail, distribution and transport
- Technology and telecoms
- Other commercial sectors
- Public sector

Interviews were conducted online in the UK (75) and the US (125) using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Key findings

The GDPR will affect organizations

- Only 46% of respondents are fully aware of the GDPR
- After learning more about it, nine in ten (90%) respondents think that the GDPR will have some impact on their business
- 89% of respondents named at least one area of their business that is being drained as a result of the GDPR

It will take time to prepare for the GDPR

- It takes an average of three months to create a GDPR compliance plan, and a further three months to implement it
- On average, plans were reviewed three times during implementation

Most organizations are not yet GDPR ready

- Around three in ten (31%) say that their organizations test practices are fully compliant
- Less than half (46%) are highly confident that their organization will be ready in time
- Only a third (33%) are very confident that every piece of customer data could be identified promptly across all systems and applications
- Around four in ten (41%) think that their data access is restricted with sufficient granularity
- Only 34% are completely confident that they could erase customer data “without delay”
- Only 43% would fully be able to provide a customer with their data in a format accessible by them and transmissible to other formats

Organizations will need to invest in technology to comply

- 88% report that there are technological challenges that present a compliance risk
- Almost nine in ten (88%) respondents realize that their organization will need to invest in new technologies or services to help them prepare for the impact of the GDPR
- 58% believe they will need to invest in encryption technologies
- 18% are not currently using synthetic data generation, but the GDPR may influence them to adopt it

Awareness of the GDPR

The European Union (EU) recently approved a new legal act – the General Data Protection Regulation (GDPR), which aims to increase the protection of personal data held by organizations. When it comes into effect in May 2018, organizations worldwide that hold personal data originating from the EU will need to be fully compliant, so it is essential organizations start acting now by reviewing the systems they use to manage data.

During the week that the GDPR was formally adopted (in April 2016), only 46% of respondents reported being fully aware of it, a further 47% had some awareness of the regulation admitting that there are gaps in their knowledge.

Impact of the GDPR on the business

It is clear that many areas of respondents' businesses will be affected by the GDPR. Once respondents were shown a definition of the GDPR, many conceded that it will have a significant impact on their organization. And at least nine in ten reported that there will be "some" impact in each area listed (figure 2).

GDPR impact

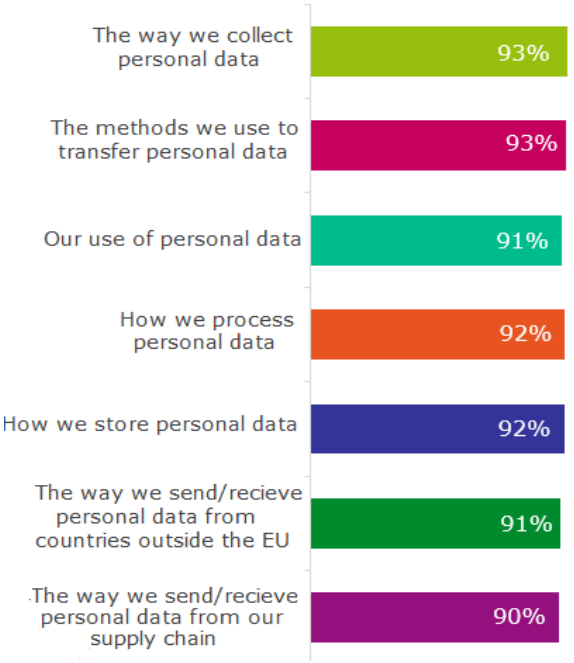

Figure 1: Analysis of respondents who say that each area will have some impact on the business. *Asked to all 200 respondents*

The higher the awareness of the GDPR among respondents, the higher the predicted impact on the business. IT decision makers (ITDMs) and risk and compliance decision makers (RCDMs) who do not yet know much about the GDPR, are yet to realize how much of an impact it will have on their organization. This knowledge is vital to ensure that organizations are able to prepare in time for the GDPR deadline (May 25th, 2018).

Changing regulations are a drain for many organizations

Almost nine in ten (89%) respondents named at least one area that is being drained in their organization as a result of the GDPR. In fact, 96% of those who are fully aware of GDPR reported a drain, compared to only 33% among those "not really" or "not at all" aware of GDPR. Where there is a lack of knowledge about the GDPR, organizations are likely to be shocked about how much they will need to do to ensure compliance.

The most likely drain reported by respondents is that IT resources and staff time (60%) will be depleted as a result of the GDPR. The IT department are much more likely to think this is the case compared to risk and compliance (66% vs. 30% respectively).

Training resources (38%) and training budgets (37%) are also likely to be affected, yet 34% of respondents will not have enough of each to enable GDPR compliance.

US vs UK

Despite it being an EU regulation, a similar proportion of respondents in the UK and US reported being fully aware of the GDPR (45% and 46% respectively).

UK respondents are more likely to consider the GDPR a strain on resources. 93% of UK respondents said keeping up to date with changing general data protection regulatory requirements - and their relevance - is a drain to some extent, compared to 87% in the US.

Preparing for the GDPR

Implementing compliance plans for GDPR

Where respondents' organizations have a full compliance plan in place, respondents report that it took their organization an average of three months to create the plan and another three months, on average, to implement it. While this is only a total of six months altogether, the majority (54%) of respondents are not highly confident that their testing alone will be compliant within the two-year implementation period.

Of those who have started (but not necessarily completed their GDPR compliance plans), respondents report having gone back and changed parts of their plan three times on average, so far. This may contribute to the 89% reporting that keeping up to date with changing general data protection regulatory requirements and their relevance is a drain on their organization.

Organizations that have not yet started creating a compliance plan need to do so soon to ensure they are compliant before the deadline.

Technological challenges in GDPR compliance

Becoming compliant with the GDPR is not going to be easy. Almost nine in ten (88%) respondents report that there are technological challenges that present a compliance risk. Over half (54%) report that sensitive data is stored inconsistently within their organization.

Respondents in the IT department (92%) are more likely to anticipate technological challenges presenting compliance risks than those within the risk and compliance department (70%). Arguably, the IT department has better sight of technological challenges, but the risk and compliance department should have a better understanding on compliance risks. Either way, it is the majority of both departments who consider there to be challenges.

Technological challenges presenting compliance risks

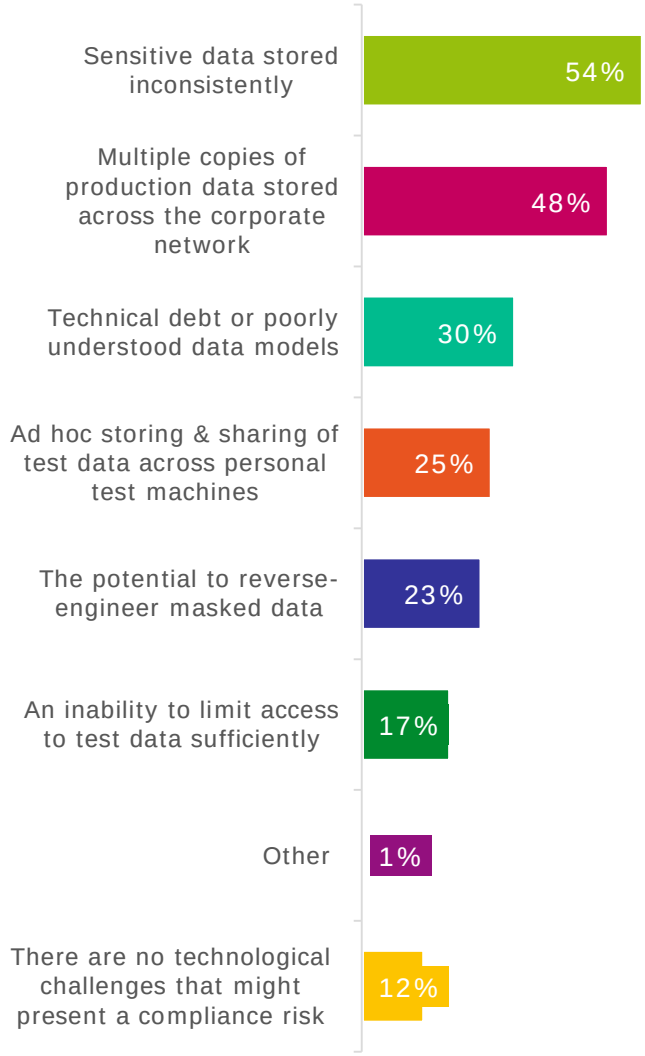

Figure 2: "Which technological challenges might present a compliance risk to your organization?" *Asked to all 200 respondents*

A high percentage of respondents (88%) reported there are technological challenges that present a compliance risk. The area presenting the highest challenge is storing sensitive data correctly (54%)

Current roadblocks to GDPR compliance

Current testing practices are not up to standard

Only three in ten (31%) respondents state that the current testing practices at their organization comply with the GDPR, from a technological, procedural and cultural perspective. The majority of organizations have a lot of work to do to ensure that they will comply. And they have less than two years to ensure that this is in place.

Current compliance

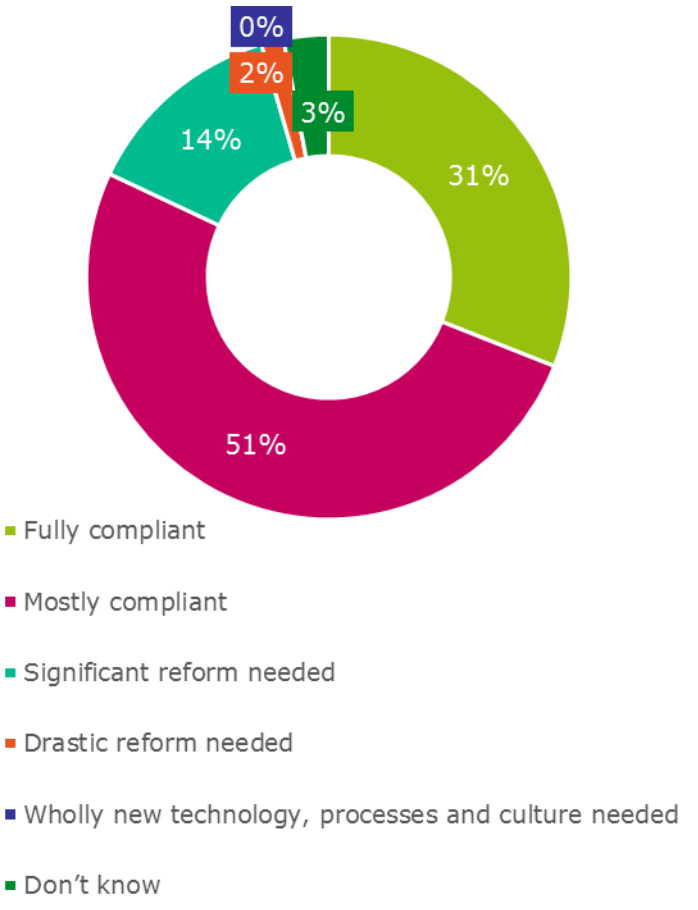

Figure 3: "To what extent do you believe that current testing practices at your organization comply with the General Data Protection Regulation, from a technological, procedural and cultural perspective?" *Asked to all 200 respondents*

However, it is under half (46%) of respondents who are highly confident that they will be compliant within the implementation period. This suggests that the majority of organizations are worried that they will not be ready to meet the May 25, 2018 deadline.

C-suite (52%) respondents are more likely to be highly confident that their organization will meet the deadline, compared to only four in ten (40%) senior managers who think that this is the case.

Throughout the research, the opinions of the C-suite and senior managers differ, and this could be because senior managers are more likely to be on the front line and are possibly more aware of the reality than the C-suite, who could be saying what they hope is true.

Compliance gaps in current processes

The processes in the majority of surveyed organizations are not compliant with the GDPR.

Only a third (33%) of respondents are very confident that every single piece of user data could be identified promptly (within ten business days) across the systems and applications that exist in their organization. This means that the majority are not very confident that their organization could do this currently. It is 42% of C-suite respondents who say that they are very confident that this could be done in their organization compared to 25% of senior managers. Are the C-suite hoping that they are already able to do this, or perhaps just unaware of what this entails?

Only 41% report that current processes and technology are capable of limiting data access to the extent required by the regulation. Again, this means that the majority are not ready for the GDPR in this area. The C-suite appear to be more likely to think that their organization is already compliant in this area, half (50%) of them say that this is the case, compared to only around three in ten (31%) of senior managers. This further suggests that the C-suite may have rose-tinted glasses on when thinking about how ready their organization is for the GDPR.

Erasing customer data “without delay”

One of the key features of the GDPR is the “Right to be Forgotten”, which gives a data subject (e.g. customers) the right to order a controller (e.g. organizations) to erase any of their personal data in certain situations.

Only around a third (34%) of respondents are completely confident that their organization can erase every instance of a customer’s (test) data without delay, if this was requested by a customer. A further 43% are somewhat confident, but do not think that they would be able to catch every piece of data, which would be against the regulation. Yet again, the majority of organizations have work to do to ensure that they will be compliant with the GDPR.

Erasing data

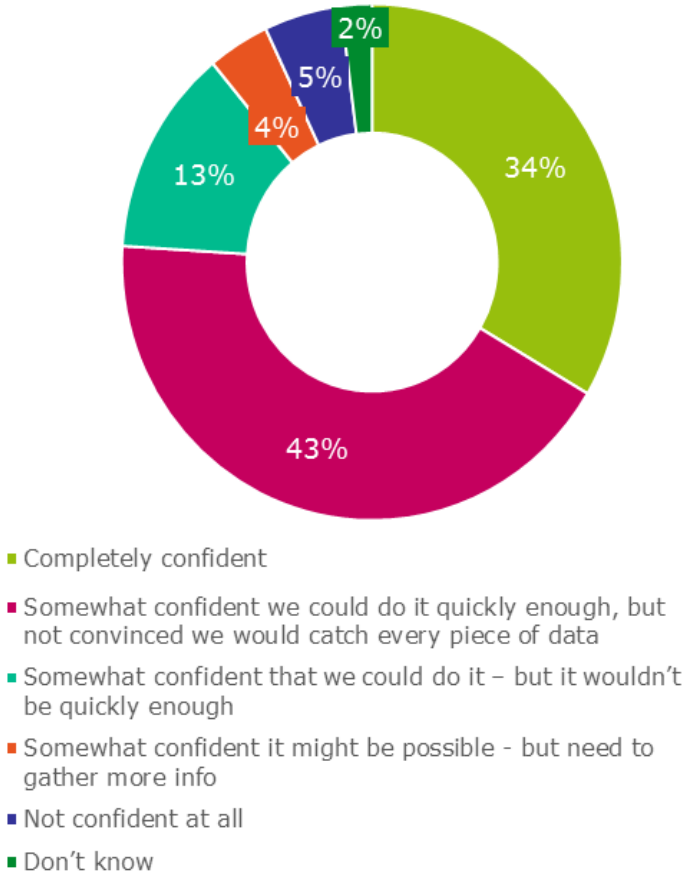

Figure 4: “If a customer requested that every instance of their personal (test) data be erased “without delay”, how confident are you that your organization is able to comply with this request at present?” *Asked to all 200 respondents*

Allowing customers access to their data

Another main feature of the GDPR is the “Right to Data Portability”; data subjects will be able to transfer their personal data between service providers, and organizations have to enable this.

If a customer requested access to every instance of their data, in a format accessible by them and transmissible to other formats, only 43% of respondents state that their organization can comply with this fully at present. A similar proportion (44%) can do this, but only in one or two formats, which may not be a format desired or even readable by the customer. A further one in ten (10%) currently have no way of doing this at all. Once again, it is evident that organizations need to change the way that they are working in order to be compliant with the GDPR.

US vs UK

US respondents are more likely than UK respondents to be confident that their organization will be ready in time, and that they are already compliant. US respondents are more likely to have:

- High confidence that testing will be compliant within the two-year implementation period - 49% of those from the US are, compared to 41% from the UK
- Very confident that every single piece of content could be identified promptly (within ten business days) across the systems and applications that exist at their organization - 38% in the US are, compared to 24% in the UK
- Data access is restricted with sufficient granularity - 44% of those in the US say this, compared to 35% in the UK
- Complete confidence they can erase every instance of personal (test) data “without delay” at present - 36% in the US say this, compared to 29% in the UK
- Can provide data in a format accessible by customers and transmissible to other formats, at present - 47% of respondents from the US say this, compared to 36% in the UK

Technologies to assist with GDPR compliance

The need for investment in technology

Almost nine in ten (88%) respondents realize that their organization will need to invest in additional technology in order to comply with the GDPR. They are planning to do so in a variety of areas including encryption technologies (58%), analytic and reporting technologies (49%) and test data management (47%).

Almost four in ten (39%) C-suite respondents predict that significant investment will be required, compared to under half that amount (16%) of senior managers who think this will be the case for their organization. This is surprising considering that C-suite respondents are more likely to think that their organization is already compliant in several areas.

Technologies to assist with compliance in test environments

Many organizations have practices in place (green in figure 5 below), or plans to put something in place (pink, below), to help ensure compliance in test environments. Although there is a proportion without plans in place yet, it is encouraging that the majority of that group know that they should do so (aqua, vs. orange).

While many have some of these in place already, it is worth remembering that almost nine in ten (88%) reported that there are technological challenges that present a compliance risk (figure 3) and over half reported that sensitive data is stored inconsistently within their organization.

Ensuring compliance in test environments

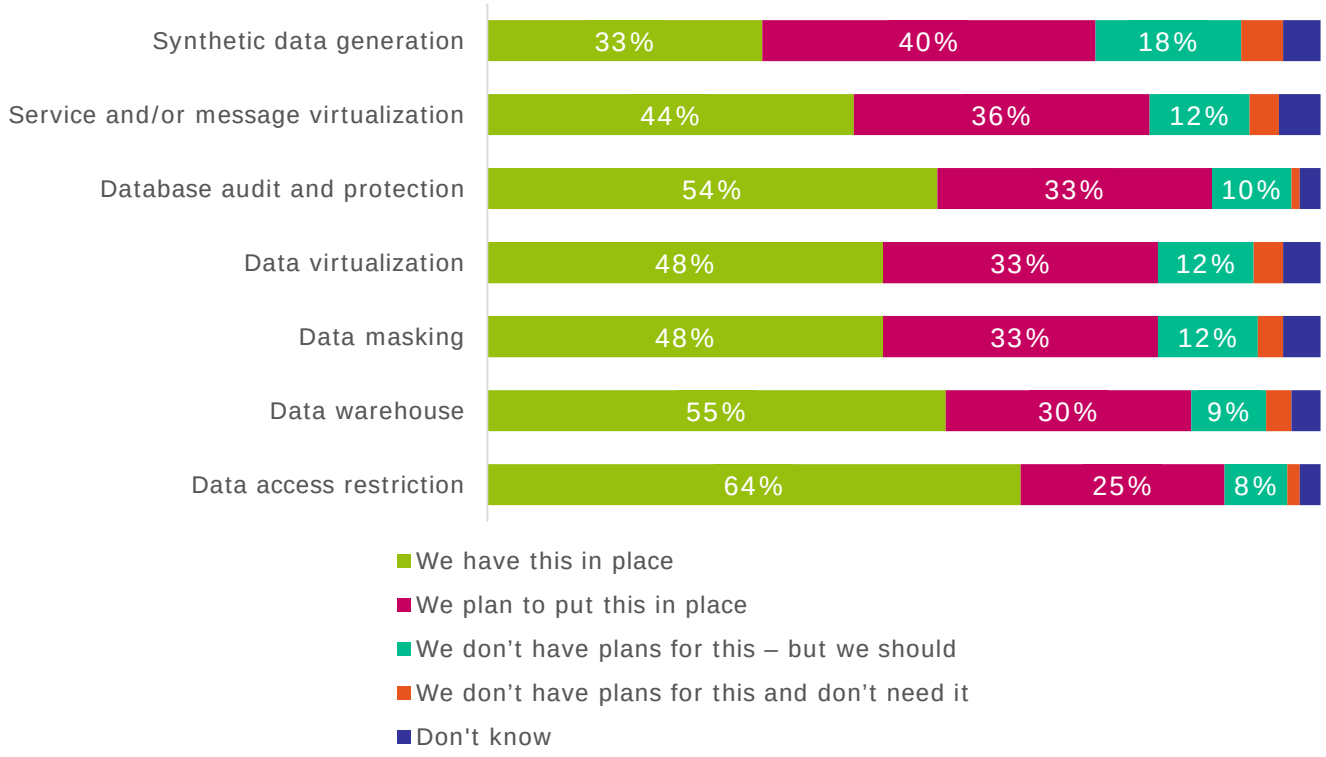

Figure 5: "What current practices are in place/do you think your organization needs to help ensure compliance in test environments?" *Asked to all 200 respondents*

Use of synthetically generated data

Only 19% of respondents' organizations use synthetically generated data (without the use of masked data as well), but a further 18% say that the GDPR might influence them to adopt it.

A data masking and synthetic data mix is going to be the most common solution for GDPR compliance

Almost six in ten (58%) respondents say that their organization will implement a combination of data masking and synthetic data generation to demonstrate compliance with the GDPR in relation to the use of personally identifiable information.

C-suite (65%) respondents are more likely to think that their organization will plan to implement a combination of data masking and synthetic data generation to demonstrate compliance. This is compared to just over half (51%) of senior managers who say their organization plans to do this.

However, 7% of respondents say that nothing has been decided or discussed when it comes to the action that their organization will take in order to comply. These organizations need to start planning to ensure that they are compliant before the deadline.

Pseudonymization

Definition: The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisation measures to ensure non-attribution to an identified or identifiable person

Of organizations who currently mask data, 13% of respondents are not aware that their organization's processes may need to be assessed in line with the GDPR. And, only 39% believe that their current processes and technologies regarding pseudonymization are up to scratch. Once again, the majority of organizations have work to do in order to be compliant with the GDPR.

And yet again, the C-suite (46%) respondents are more likely to think that their organization is already compliant in this area, compared to 31% of senior managers who think this.

Those with a higher level of GDPR awareness are more likely to say that their organization is currently up to scratch. Those with better GDPR awareness may have already taken action within their organization to prepare for compliance.

US vs UK

US respondents are more likely to agree that significant investment will be required (31% of those in the US agree, compared to 20% in the UK).

However, 15% of those in the UK will switch from data masking to synthetic data generation to avoid the use of any production data, compared to 7% in the US.

Conclusions

Considering that the GDPR was only formally announced recently, there is a fair level of understanding amongst respondents. Once informed about the regulation, 88% reported that their organization faces technological challenges in becoming GDPR compliant. There is a realization that a lot of work is needed to become compliant.

Many respondents have revealed gaps in GDPR compliance within their organizations at present. Considering the realization that there will be technological challenges, it is no surprise that 88% need to invest in technologies in order to comply with the GDPR. Encryption technologies will be invested in by 58% and a considerable proportion think that the GDPR might influence them to adopt other technologies like synthetic data generation within a test data management solution (18%).

Changing GDPR requirements are a drain to respondents' organizations; preparations are underway for some, but there is still a lot to do. It takes six months to plan and implement for the GDPR (plus revisions). If organizations do not start to create a compliance plan soon, they may run out of time before the deadline in May 2018.

There is education to be done around the new regulation itself - as well as assistance required with technologies. As in every case, it is only the minority who are either confident in their organizations' processes, or reporting that their organization is already compliant with elements of the GDPR. Only 31% think that their organization is fully compliant in regards to current testing practices. And only 39% think that their current policies regarding pseudonymization are up to scratch. The majority of organizations have work to do to ensure compliance.

Even though the GDPR is a European regulation, US organizations are bracing for impact. The regulation will affect organizations globally, so it is no wonder that 31% of those in the US agree that significant investment in technologies will be required to assist with GDPR compliance.

All organizations should be putting plans in place to become GDPR compliant, before it is too late.

If you would like to hear more about the GDPR and the actions your organization could take, view the CA and Vanson Bourne webcast:

"Are You GDPR Ready? Get the Vanson Bourne Readiness Survey Results"

About CA:

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

CS200-215379

About Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Our reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com