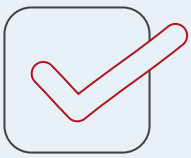
2017 VERITAS GDPR REPORT

Chapter 2: Think your organization is ready for the GDPR? Think again...

VERITAS™

The truth in information.

The one year marker has already passed, with the clock ticking for organizations to become GDPR compliant. This looming deadline may not concern many organizations, as **31%** of those recently surveyed think their enterprise is already GDPR compliant. But, it's highly possible those very organizations are relying on false hopes or a sense of preparedness that is too good to be true.



Experts took time to analyze the results from the 2017 Veritas GDPR Report to find that only **2%** of respondents actually appear to be compliant. Upon closer inspection, worryingly this suggests that in fact almost all organizations are not ready, even if almost a third of those surveyed think that they are today.

The statistics referenced in the remainder of this report are based on those that stated their organization is already GDPR compliant.

Where are organizations going wrong?

This report looks to highlight the vital areas where organizations who stated they are compliant still have a lot of work to do to ensure GDPR compliance, before May 2018, to avoid the high fines that come with non-compliance.

Fail to prepare, prepare to fail

GDPR requires that organizations ensure appropriate technological protection and organizational measures are implemented to be able to immediately establish if a personal data breach has taken place. Yet, almost half (48%) of respondents who stated their organizations are GDPR compliant admit that they do not have full visibility over identifying personal data loss incidents.

Without full visibility, how can they ensure that a breach is reported to the supervisory authority within 72 hours, and inform the individual affected without undue delay – as mandated by GDPR?

The answer is that they currently can't. More than 60% of those that say they are ready for GDPR admit that it is difficult for their organization to identify and report a personal data breach within 72 hours. Failing to do this could be classified as a major violation of the regulation and the fines in these cases are up to 4% of annual revenue or up to 20 million EUR.

Difficulty identifying and reporting a data breach within 72 hours

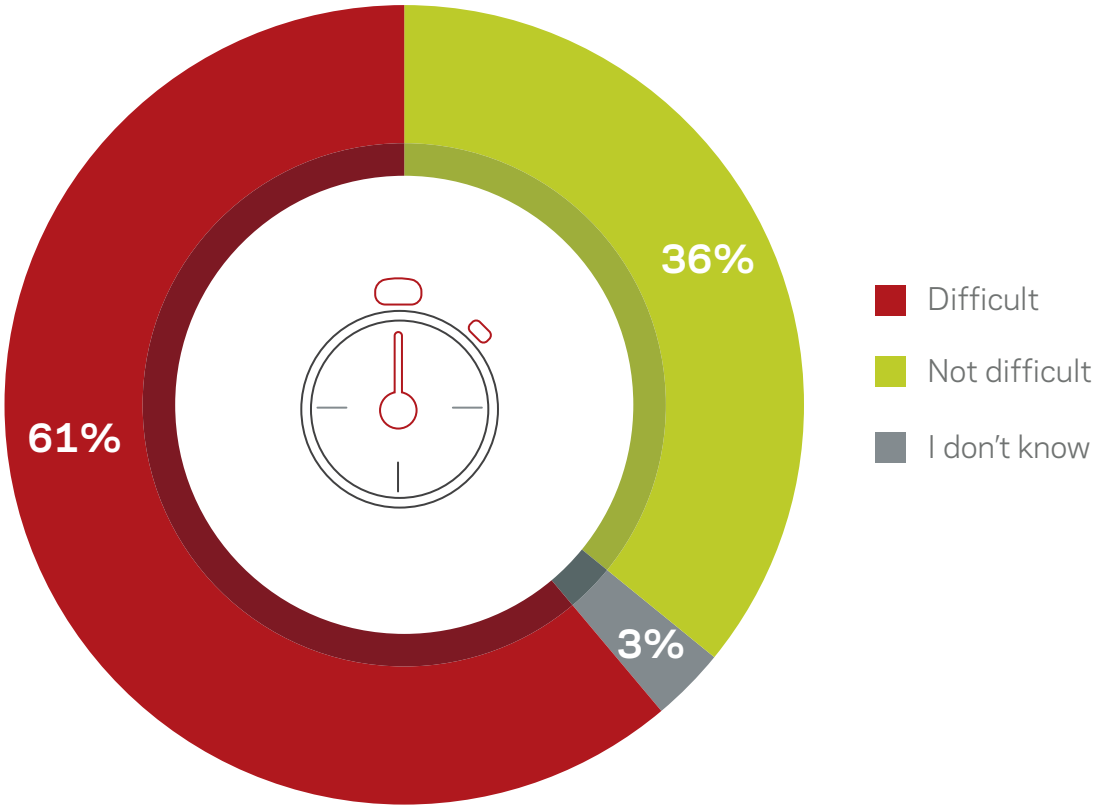


Figure 1: "How difficult is it for your organization to identify and report a data breach within 72 hours?" Showing the results of the 279 respondents who think that their organization is already GDPR compliant

Departing employees and data theft: a struggle from within

Once an employee leaves an organization their rights to access company data are usually withdrawn. But, incredibly, half (50%) of respondents who say their company is compliant also admit that former employees can still access company data.

With this type of uncontrolled access, many organizations are leaving themselves open to the risk of an attack from former employees or, equally as alarming, putting confidential information in the hands of people who shouldn't have it, which would infringe on GDPR compliance. Existing employees could also be a risk as organizations struggle to keep on top of internal threats. As many as six in ten (60%) respondents admit that their organization does not have full visibility over monitoring internal threats to personal data.

It may be assumed that threats from existing employees are low, but the risk could be higher amongst former employees.

Their ability to access any company data must be stopped as soon as they leave, and ideally restricted as soon as their notice is given.

The blame game: data stored in the cloud – who is responsible

Cloud use in organizations is ever increasing. The vast majority (94%) of respondents who say that their organization is already compliant use hybrid cloud, where data is stored both on-premises and in a public or private cloud environment. For many of these organizations, the data stored in the cloud will need to comply with the GDPR. Almost half (49%) of respondents who say they are ready for the upcoming regulation believe that their organization's cloud service provider (CSP) is solely responsible for the GDPR compliance of their data stored in the cloud. But unfortunately, these organizations are wrong. It is the responsibility of the organization as the data controller to ensure that the data processor (in this

Former employees of my organization are able to access company data

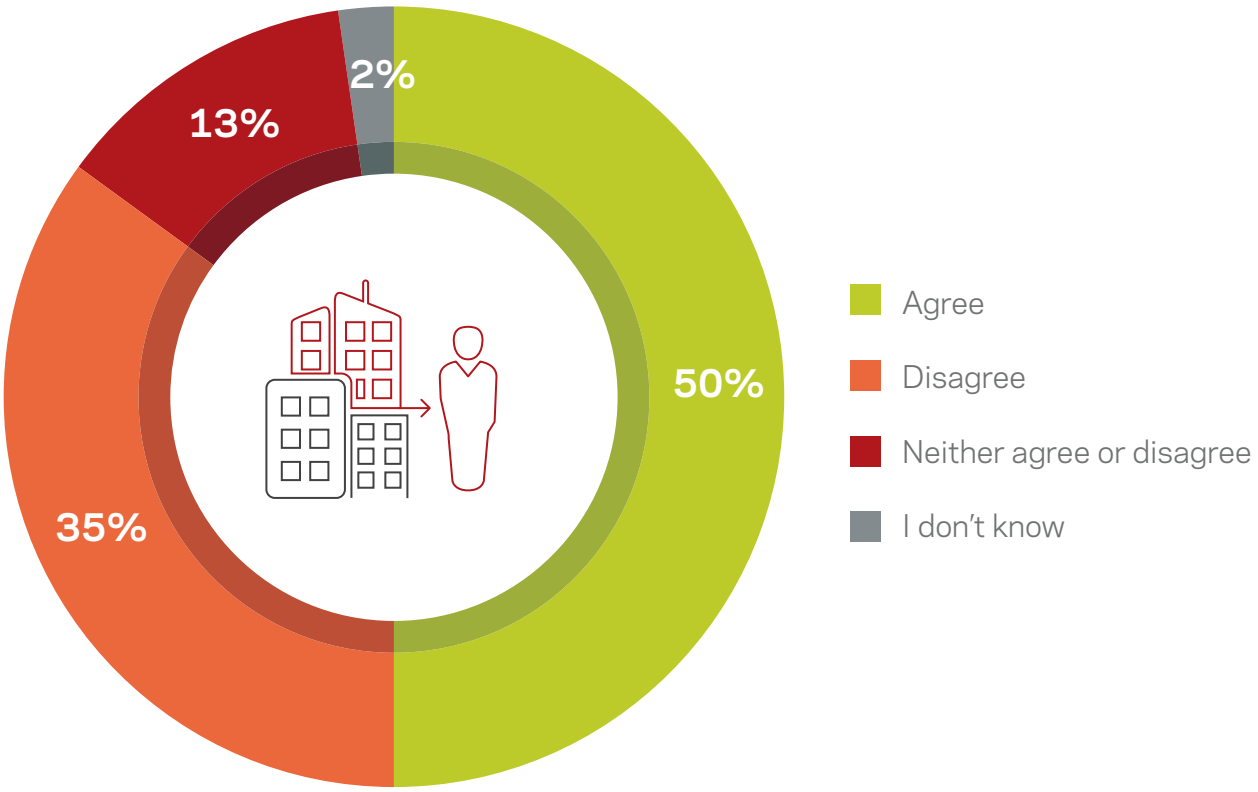


Figure 2: "To what extent do you agree or disagree with the following? Former employees of my organization are able to access company data"
Showing the results of the 279 respondents who think that their organization is already GDPR compliant

case the CSP) provides sufficient guarantees of being GDPR compliant. This means that both the CSP and the organization are responsible for ensuring data compliance in the cloud. Organizations need to understand that they cannot pass the buck to the CSP. This false sense of protection could cost organizations millions and lead to permanent brand damage if and when issues arise.

With a right to forget, the challenge is set

In January, the EU will be launching a campaign to inform citizens of their new rights under the GDPR. This is likely to empower consumers to ask organizations to remove all instances of their data, no matter where it is stored. The data could be stored in a clearly defined database, but it may also be duplicated, in an excel document on the network, or on an employee's device for example. Nearly 20% of respondents who are confident they are GDPR compliant also admit that personal data held within their organization cannot be purged or modified. Not only that, some can't search data, don't know where it is or do not have data clearly defined. More than one in ten (13%) respondents admit that their organization…

- …does not have the capability to effectively search and analyze personal data to uncover both explicit and implicit references to an individual
- …does not have accurate visibility into where all of their data is stored
- …or, admit that their organization's data sources and repositories are not clearly defined

This means that many organizations will not be able to easily search, find and erase their customers' data if/when they exercise their "right to be forgotten", which risks a key violation of the GDPR. Organizations need to ensure that they can do this for any data they hold, while at the same time, minimising the data that they process, so that it is only used for the purposes it has been collected for.

There are many aspects that organizations need to firm up to ensure GDPR compliance. Enabling the organization to identify and respond to a breach immediately, ensuring that former employees cannot access company data, retaining responsibility for data held within the cloud and being able to react to requests to be forgotten are just a handful of examples of where organizations need to make drastic improvements to become GDPR-ready.

For information on how Veritas Technologies can help your organization become GDPR compliant visit:

veritas.com/gdpr

Methodology

Veritas commissioned independent technology market research specialist Vanson Bourne to undertake the research upon which this report is based.

A total of 900 business decision makers were interviewed in February and March 2017 across the US, the UK, France, Germany, Australia, Singapore, Japan and the Republic of Korea. The respondents were from organizations with at least 1,000 employees, and could be from any sector. To qualify for the research, respondents had to be from organizations who do at least some business within the EU.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates had the opportunity to participate.

VERITAS™

The truth in information.