

Forrester Opportunity Snapshot: A Custom Study Commissioned By IBM | May 2018

# Benchmark Your Readiness For A GDPR-Compliant World

How The Right Tools And Strategies Can Help Companies Reap Business Benefits Through Sustained GDPR Compliance

GET STARTED ►



# Benchmark Your Readiness For A GDPR-Compliant World

## OVERVIEW

## SITUATION

## APPROACH

## OPPORTUNITY

## CONCLUSIONS

## Overview

The EU General Data Protection Regulation (GDPR) has arrived. Every company doing business with European customers — regardless of location — must make considerable governance, people, process, and technology changes to comply with the new rules. While companies have made progress, more work remains. To succeed, they must tackle key challenges, including data identification, mapping, and access management. Despite the work ahead, forward-looking businesses understand GDPR is an opportunity. This is a transformation for a data-savvy world, with the potential to yield enhanced customer and business benefits. Investment in solutions with data privacy, security, and compliance offerings that can protect data no matter where it's stored — on-premises and in the cloud — can ease companies along their readiness journeys and help them achieve and sustain compliance from May 25, 2018, and onward.

In February 2018, IBM commissioned Forrester Consulting to survey 163 business and technology leaders involved in their companies' GDPR, compliance, and data protection decisions to examine their level of GDPR readiness and understand what they require for sustained GDPR compliance.

*To participate in the study, respondents had to work at companies with at least 250 employees, serve European customers, and process large volumes of personal data as part of their operations.*



### Country

- > **31%** United States
- > **18%** Nordics
- > **18%** France
- > **17%** Germany
- > **17%** United Kingdom



### Number of employees

- > **16%** 250 to 499
- > **21%** 500 to 999
- > **27%** 1,000 to 4,999
- > **36%** 5,000 or more



### Seniority

- > **13%** C-level executive
- > **32%** Vice president
- > **29%** Director
- > **25%** Manager



### Top industries

- > **17%** Financial services
- > **15%** Retail
- > **13%** Travel and hospitality
- > **9%** Manufacturing

*Note: Percentages may not total 100 because of rounding.*

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

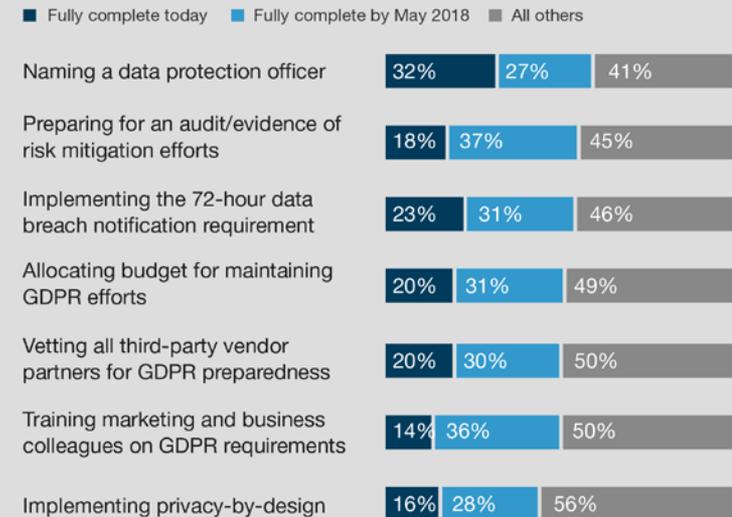
## For Many, Much Of The Work Toward GDPR Compliance Still Lies Ahead

Come May 25, 2018, regulators will start enforcing GDPR. To comply with the new requirements, organizations need to radically transform their handling of personal data.

Organizations report progress, but considerable work remains. Just two months ahead of the deadline, 32% or less report completion of key initiatives; between 41% and 56% expect to miss the deadline on these efforts. Just over half of firms expect to name a data protection officer (DPO), to be prepared to provide evidence of risk mitigation efforts in the event of an audit, and to have implemented the 72-hour breach notification requirement. However, just half or less expect to successfully tackle requirements that demand greater changes to firms' processes, such as implementing privacy-by-design and vetting third parties for GDPR preparedness.

As a result, 61% are "very" or "extremely" concerned about their firm's ongoing ability to meet regulator expectations after the deadline. Further, 51% are concerned about meeting the expectations of the ultimate stakeholder: the customer.

"For each of the following GDPR initiatives, please indicate where your organization is with implementation."



Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

## Sustained Compliance Requires Continuous Diligence

Respondents anticipate a range of challenges after the enforcement deadline, the greatest of which include:

- › **Continuously identifying and classifying data.** To protect data, firms must first know where it's stored and its risk profile. Yet, 45% expect to be challenged by obtaining this kind of ongoing visibility.
- › **Governing data access.** Today's digital landscape is causing organizations to generate, store, and transmit massive amounts of data, much of it sensitive. Firms must ensure access to this data is in line with business need and risk objectives.<sup>1</sup> But challenges with data access — internally and externally — will persist for many.
- › **Executing on timely breach notification and response.** The GDPR gives firms a mere 72 hours from the moment they become aware of a data compromise to notify customers and authorities. Thirty-nine percent expect to struggle with this requirement.
- › **Running data protection impact assessments.** Regardless of whether a breach has occurred, regulators may require firms to demonstrate evidence of their risk mitigation efforts. To meet that need, firms must run data protection impact assessments (PIAs) — something over a third say will be a challenge after May.<sup>2</sup>

“Which of the following are challenges you anticipate for your organization after GDPR takes effect?”

(Select all that apply; showing top challenges)



Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

## Noncompliance Threatens Brand Reputation And Customer Trust

With the work ahead, it's not surprising that just 54% of leaders express high confidence in their ability to address an ad hoc audit after the deadline. This is troublesome considering they also associate great risk with noncompliance. Regulatory fines — which can amount to 4% of annual revenue or €20 million, whichever is greater — are a key, but not primary, concern.

Instead, leaders are most worried about the impact of enforcement action, which can mean additional security requirements and a loss of operational control. Data-savvy companies understand that customers will only engage with firms they trust with their data, and they rightly use customer privacy as a source of competitive differentiation and brand value. This helps explain why concerns over long-lasting negative effects on the company's brand and on customer trust are top-of-mind for GDPR decision makers.

*Fifty-three percent are concerned about diminished customer trust should they be found to be noncompliant.*



“How concerned are you about these consequences if your firm fails to meet GDPR requirements after the legislation goes into effect?”



Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

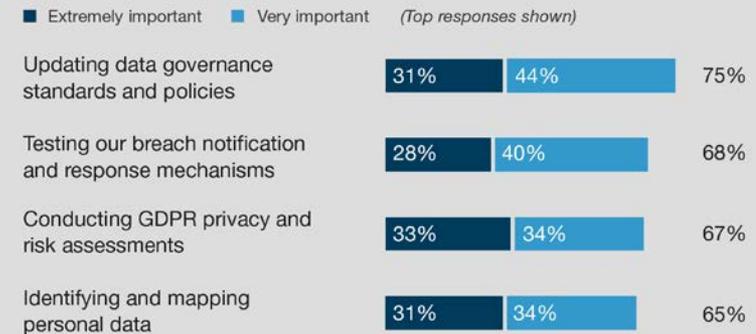
1 2

## Data Governance Plays A Pivotal Role In Getting Firms GDPR-Ready

Decision makers are taking a diverse set of actions to meet GDPR requirements. Over half of respondents described all ten tactics we tested as “extremely” or “very” important in their readiness efforts. However, firms mainly focused on four for establishing readiness: updating data governance standards and policies, testing breach notification and response mechanisms, conducting PIAs, and identifying and mapping personal data.

But most of all, the GDPR deadline is forcing organizations to revisit and modernize their data governance practices. Developing these capabilities will be essential for the safe flow of data inside and outside the organization. These capabilities will also be important for meeting new rules around managing customer consent, which include addressing data subject rights such as customer requests for data portability or data deletion.

“How important a role did the following initiatives play in your organization's efforts to establish GDPR compliance?”



Note: Showing “5” and “4” on 5-point scale where 5 is “Extremely important” and 1 is “Not at all important”

Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

*Improved data governance practices will be important for delivering on GDPR requirements related to managing customer consent.*



# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

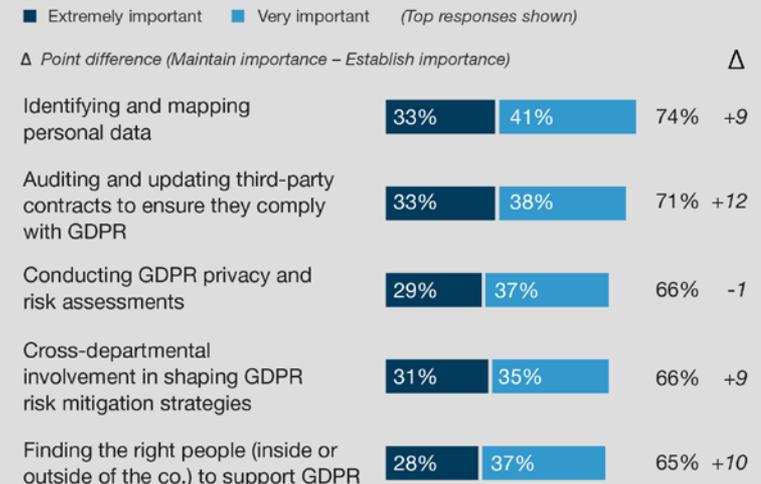
1 2

## Firms Need Competence In Four Key Areas For Long-Term GDPR Success

After May 2018, much of the GDPR media attention will fade, but the work being done within companies will not. As firms achieve acceptable levels of readiness, their focus will turn to tactics for sustained compliance. Some initiatives considered important to establishing compliance — like conducting PIAs — will be just as important after the deadline; others will be even *more* important:

- Identifying and mapping personal data.** Respondents regard ongoing data identification/mapping — already a top readiness focus area — to be most important for compliance maintenance.
- Auditing and updating third-party contracts.** Third-party relationships are critical, but GDPR increases their risk. To remain compliant, firms need third-party data handling and security practices explicitly stated in contracts.
- Cross-departmental involvement in shaping GDPR strategies.** Protecting data is a companywide effort. Cross-departmental input in GDPR strategies promotes a shared privacy responsibility culture that will be important to long-term compliance.
- Finding the right people.** Firms will need to locate additional human resources beyond the DPO to support compliance.

“How important a role did the following initiatives play in your organization's efforts to maintain GDPR compliance?”



Note: Showing “5” and “4” on 5-point scale where 5 is “Extremely important” and 1 is “Not at all important”

Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

## Sustained GDPR Compliance Delivers Both Customer And Business Benefits

Sustained GDPR compliance is important, and cost avoidance is only one reason. In fact, 98% of respondents in our study agree that compliance affords companies several key benefits.

Customer-focused benefits — including enhanced customer trust and experience (CX) — top the list. As recent data breaches have put a strain on the trust customers have in firms handling their data, companies must offer additional assurances and reasons to do business with them.<sup>4</sup> GDPR presents an opportunity to update customer-focused communication around managing consent and companies' commitment to privacy with an eye toward promoting transparency. These efforts build trust and can improve CX.

*Ninety-eight percent expect business benefits through sustained GDPR compliance.*



### “What business benefits would you expect to realize through sustained GDPR compliance?”

*(Select all that apply)*



Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

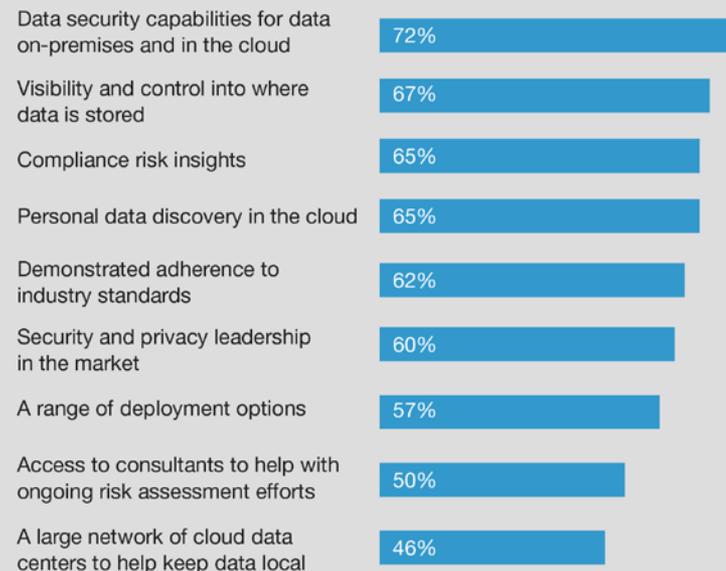
## Organizations Value Partners Providing Holistic Data Protection And Visibility

Companies find value in several capabilities partners might provide to help them remain GDPR compliant. With increased adoption of software-as-a-service (SaaS) applications and use of the cloud for data storage, backup, and protection, it comes as no surprise that security tools that can protect data on-premises and in the cloud are especially valued. Visibility and control into where data is stored, compliance risk insights (tools that identify compliance risk to sensitive data), and personal data discovery in the cloud are also highly valued. Sixty-two percent say it's important for partners to adhere to industry standards. Achieving compliance with industry-specific mandates (HIPAA, PCI) may be less expensive with cloud providers, which often have superior security capabilities that can scale.<sup>5</sup>

While firms may be maturing in their adoption of cloud services to deprioritize the location of the data center (46% described as extremely/very important) in favor of security controls (72% described as extremely/very important), a large network of data centers has the advantage of addressing customer concerns — real or perceived — around personal data. In Forrester's experience, customers are more comfortable when their data stays close to home, even when regulators don't require it.<sup>6</sup>

"When evaluating partners that process personal data on your behalf, how important are the following capabilities they may offer in helping your organization maintain GDPR compliance?"

Showing "Extremely important" and "Very important"



Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

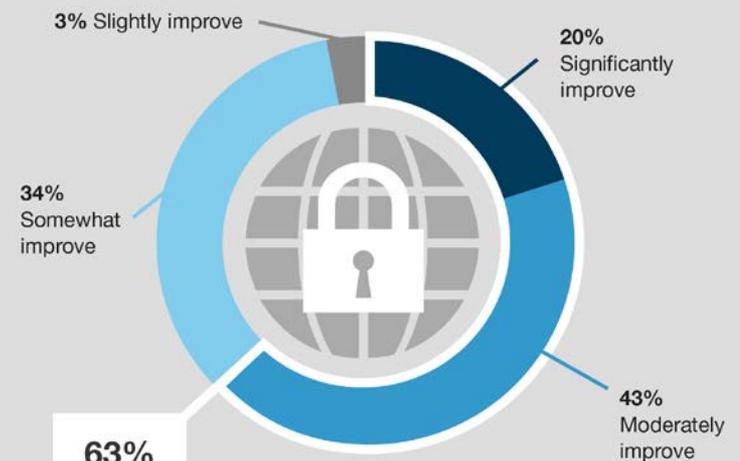
1 2 3

## Partners Can Help Organizations Along Their GDPR Compliance Journey

Organizations must own GDPR compliance, but they recognize that partners with data privacy, security, and compliance offerings can ease their GDPR compliance journey and help them promote a stronger security and privacy posture. Sixty-three percent agree that if a services partner that processed personal data on their behalf could offer the following capabilities, it would moderately or significantly improve their ability to maintain GDPR compliance:

- › Data security capabilities that can protect data on-premises and in the cloud.
- › Visibility and control into where data is stored.
- › Compliance risk insights.
- › Personal data discovery in the cloud.
- › Demonstrated adherence to industry standards/auditor guidelines.
- › Security and privacy leadership in the market.
- › A range of deployment options.
- › Access to consultants to help with ongoing risk assessment efforts.
- › A large network of cloud data centers to help keep data local.

“If a services partner that processed personal data on your behalf could provide you all of these capabilities, what impact would that have on your ability to maintain GDPR compliance?”



Base: 163 professionals with responsibility or influence over GDPR, compliance, and data protection decisions at their companies  
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, March 2018

# Benchmark Your Readiness For A GDPR-Compliant World

[OVERVIEW](#)[SITUATION](#)[APPROACH](#)[OPPORTUNITY](#)[CONCLUSIONS](#)

## Conclusion

Organizations need to make radical governance, people, process, and technology changes to comply with GDPR. They've made progress, but they must make more. Achieving GDPR compliance doesn't grant firms the ability to remain compliant over time. Sustained GDPR compliance is an ongoing journey that requires an adjustment to compliance strategies after the enforcement deadline. This includes dynamically identifying and classifying data, governing how third parties access and process data on an ongoing basis, and assessing GDPR risks holistically and continuously.

Ultimately, firms must build risk mitigation strategies that rely on flexible processes and governance, where people's skills and technology are the foundation. At a time when organizations are looking to digitally transform, adoption of cloud services — which enable new customer engagement strategies and sources of data — takes on importance but can also complicate data governance. Partners that can help organizations manage the spread of their infrastructure and safeguard data no matter where it resides can ease compliance efforts and allow them to extract data insights while retaining — and enhancing — their customers' trust.



### ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit [forrester.com/consulting](https://forrester.com/consulting).

© 2018, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [forrester.com](https://forrester.com). [E-38255]

# Benchmark Your Readiness For A GDPR-Compliant World

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

## METHODOLOGY

This Opportunity Snapshot was commissioned by IBM. To create this Snapshot, Forrester conducted a custom survey of 163 decision makers involved in their company's GDPR, compliance, and data protection decisions. Respondents had to work at companies with at least 250 employees, serve European customers, and process large volumes of personal data as part of their operations to qualify.

## REFERENCES

- <sup>1</sup> Source: "Assess Your Data Privacy Practices With The Forrester Privacy And GDPR Maturity Model," Forrester Research, Inc. April 21, 2017.
- <sup>2</sup> Source: "Create Your Cloud Security Strategy And Road Map," Forrester Research, Inc., September 14, 2016.
- <sup>3</sup> Source: "Public Clouds Spread Across Europe," Forrester Research, Inc., January 18, 2017.
- <sup>4</sup> Source: "The Future Of Data Security And Privacy: Growth And Competitive Differentiation," Forrester Research, Inc., October 25, 2017.
- <sup>5</sup> Source: "Create Your Cloud Security Strategy And Road Map," Forrester Research, Inc., September 14, 2016.
- <sup>6</sup> Source: "Public Clouds Spread Across Europe," Forrester Research, Inc., January 18, 2017.

### Project Director

Sophia Christakis  
Market Impact Consultant

### Contributing Research

Forrester's Security & Risk  
research group

## ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit [forrester.com/consulting](http://forrester.com/consulting).

© 2018, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to [forrester.com](http://forrester.com). [E-38255]