# The State Of GDPR Readiness

**GDPR Readiness Progresses, But Strategies Depend Too Heavily On IT**

by Enza Iannopollo

January 31, 2018

## Why Read This Report

With the deadline for GDPR compliance looming in May 2018, it's a good time for security and privacy professionals to take stock of how their readiness efforts and approaches compare to the rest of the industry. This data-driven report outlines the current state of compliance, trends by industry and geography, and key Forrester recommendations for moving your efforts forward.

## Key Takeaways

**GDPR Preparation Is Underway**

Despite hundreds of headlines suggesting the opposite, firms around the world are getting ready for GDPR. Many say that they are ready today.

**Maturity And Approach Vary By Industry**

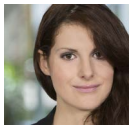
Industry-specific trends emerge. Firms in less-regulated verticals have more work to do to meet GDPR requirements. Financial services are the most mature.

**GDPR Compliance Requires A Holistic Approach**

While security and privacy pros are approaching GDPR by tackling individual requirements, they find it very challenging to design and execute a comprehensive compliance program. But, this is necessary to deliver meaningful — not just formal — compliance.

# The State Of GDPR Readiness

## GDPR Readiness Progresses, But Strategies Depend Too Heavily On IT



by Enza Iannopollo
with Laura Koetzle, Stephanie Balaouras, Elsa Pikulik, and Peggy Dostie

January 31, 2018

## Table Of Contents



## Related Research Documents

Digital Advertising Under GDPR Hinges On Data Management

The Five Milestones To GDPR Success

TechRadar™: Data Security And Privacy, Q4 2017



FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

## GDPR Compliance Programs Are Underway Globally

With a few months left before European regulators start enforcing the EU's General Data Protection Regulation (GDPR), firms around the world are getting ready for the new requirements.[1] While the headlines of the last six months tormented us with the news that companies are largely and deeply unprepared for GDPR, our data shows a more encouraging — and complex — picture.[2]

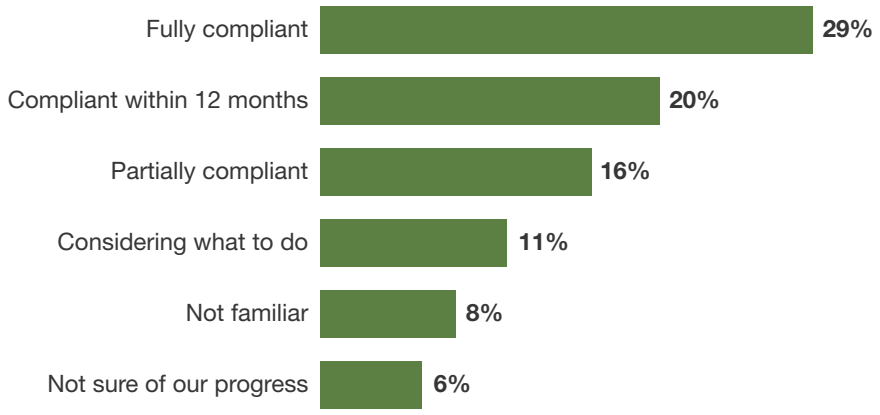
### There Is Good Progress, But There Are Also Missteps, And A Lack Of Awareness Persists

Whether running a substantial compliance program or just making small adjustments, many firms worldwide are working toward GDPR compliance, and data from the Forrester global data security survey shows that:

- **One in three firms believes they are GDPR-compliant today — but they may not be.** Our data shows that nearly 30% of companies globally are fully GDPR-compliant today.[3] However, based on our qualitative research, we believe that just a portion of these firms have actually engaged in data discovery and classification exercises as well as built data flow maps and run gap analysis. Instead, many firms have taken a piecemeal approach to GDPR, which is mainly focused on requirements that rely primarily on IT to meet specific compliance requirements, such as the requirements for data breach notification. These approaches are short-sighted, and most likely will need radical revision after the enforcement of GDPR rules start in May (see Figure 1).
- **European companies are the most pessimistic about their readiness.** In Europe, 26% of firms report that they are fully GDPR-compliant.[4] This number is the smallest across geos; nonetheless, it's still high. As we consider this evidence, we also must bear in mind that GDPR is a principle-based regulation, and to determine whether they are compliant, companies must judge whether their risk mitigation strategies are effective and in line with GDPR requirements. In many cases, this is not a simple black-or-white assessment. To make this even more difficult, also consider that many firms still find the interpretation of many GDPR requirements unclear today. Our data shows that another 22% of European firms expect to be GDPR-compliant within 12 months (see Figure 2).[5]
- **Too many firms still believe that GDPR doesn't apply to them.** GDPR has extraterritorial effect. This means that companies that are not physically present in the EU have to comply with the rules. In particular, if firms sell products or services to the European market, or if they collect data on Europeans to build profiles, for example, they fall within the scope of the rules. GDPR applies to companies that directly engage in data collection and that define the guidelines for processing activities as well as to firms that process data on behalf of their clients and strictly follow their directions. Therefore, the percentage of companies not affected by GDPR is small. Unfortunately, our data suggests that more guidance is necessary to help firms correctly access their status under the new rules (see Figure 3).

**FIGURE 1** Many Global Security Decision Makers Are Not Yet Compliant With GDPR

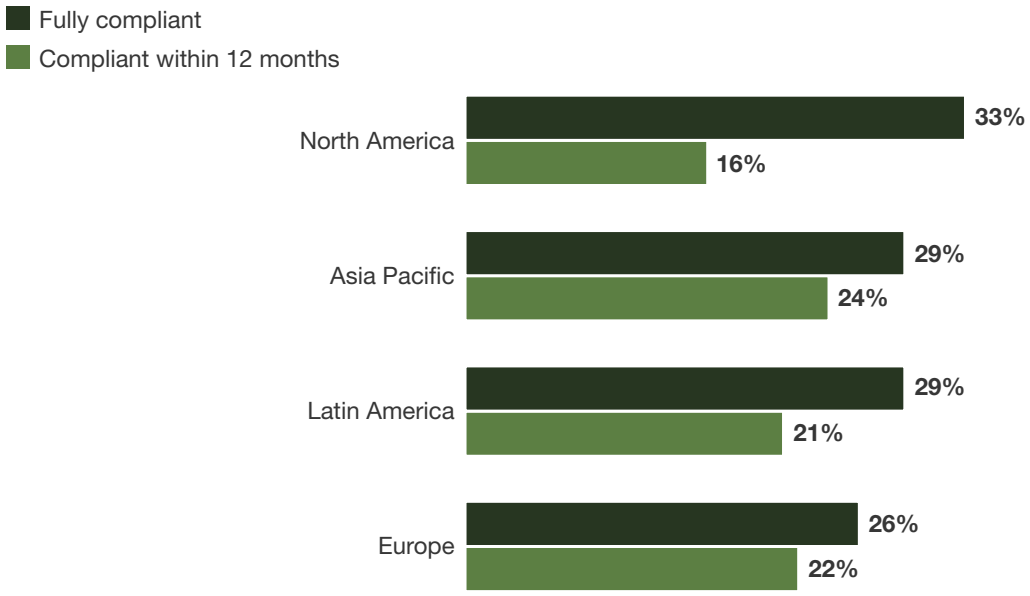
**"Which of the following best describes your firm's progress on GDPR compliance efforts?"**




Base: 3,195 global security decision makers at the manager level or above at firms with 20 or more employees
Note: "Not applicable" responses have been omitted.
Source: Forrester Data Global Business Technographics® Security Survey, 2017

**FIGURE 2** Europe Represents The Smallest Percentage Of GDPR Decision Makers Fully Compliant With GDPR

**"Which of the following best describes your firm's progress on GDPR compliance efforts?"**




Base: 200 to 1,143 security decision makers at the manager level or above at companies with 20 or more employees
Source: Forrester Data Global Business Technographics® Security Survey, 2017

**FIGURE 3** GDPR Approaches Vary Across Verticals


## Maturity Varies By Industry, And Most Firms Struggle With Process

A deeper analysis of the data, combined with our qualitative research of the last 12 months, highlights multiple challenges in companies' journey to GDPR compliance.

### GDPR Approaches And Maturity Vary Widely By Vertical And Prior Regulatory Expertise

While GDPR requirements apply to companies of all verticals (even public sector organizations), our data shows that some firms have much more advanced GDPR projects today. We've also found that the manner in which companies tackle the regulation diverges depending on factors such as whether they've had exposure to other kinds of regulatory requirements and the complexity of their processing activities. Specifically, we found that:

› **Firms in regulated industries have a head start on the GDPR journey.** Prior experience with tough regulation matters when it comes to GDPR. For example, firms in highly regulated verticals, such as financial services, have the luxury of relying on established compliance and data protection teams and often also on data protection officers — teams and individuals they put in place long before the EU finalized GDPR. It means that early on, they went straight into the definition of specific data-driven risks to mitigate in compliance with GDPR. Analytics projects on transactional customer data, for example, were at the top of their lists.[6] Conversely, for firms not used to regulation, their GDPR journeys must start with the creation of the right team that can then define a framework for the firm's compliance strategy (see Figure 4).

- **Financial services firms are the most GDPR mature.** Companies in financial services across geographies are the most GDPR mature organizations today.[7] It's not only the threat of huge financial penalties that drives these firms — GDPR is a threat to future business models if they don't get it right now. Banks manage a great deal of customer data, and many of them are using this to evolve their business models and generate new sources of revenue beyond their traditional banking services. Failure to comply with GDPR creates the potential for invasive regulatory enforcement actions that could, for example, limit their ability to process customer data in certain ways. It also means great reputational damage and loss of trust that might lead their customers to take their business and their data somewhere else.
- **Media and retail lag behind other industries.** Companies in media and retail have an enormous real estate worth of customers' (and employees') personal data to rationalize and bring within GDPR compliance. They have only just recently started their GDPR journeys, often under the pressure of their own customers. Typically, firms in these verticals approach GDPR by prioritizing data-driven activities that relate to direct marketing, personalization, and customer profiling.[8] Within these activities, the focus is on ensuring compliance with rules regarding consent and data subject rights, such as the right to be forgotten and third-party management. However, like all other firms, it's still critical for these companies to start with data discovery and classification and the identification of data-driven risks.

**FIGURE 4** GDPR Maturity Explained

**"How would you describe your firm's progress on each of the following GDPR requirements?"**

| | Chief privacy officer | 72-hour data breach notification | Privacy by design | Evidence of risk mitigation strategies | Training and awareness | Allocated budget for GDPR | Third-party vendor partners risk management |
|---|---|---|---|---|---|---|---|
| We have fully met this requirement. | ● | | | | | | |
| We are currently working on meeting this requirement. | | ● | | | | ● | |
| We are making plans on how to best meet this requirement. | | | ● | ● | | | |
| We have not begun to address this requirement. | | | | | ● | | ● |

## Firms Consistently Struggle To Comply With Process-Based Requirements

Too many organizations today rely mainly on technology to tackle GDPR compliance. Our research shows that adopting security controls such as encryption and tokenization, as well as acquiring controls for network security, tops the list of GDPR-related priorities. As a result, firms are neglecting requirements that hinge more heavily on processes, such as managing data subject rights and consent management. This is worrisome because:

› **Firms are hiring CPOs, but they are not GDPR decision makers.** Many firms have hired a data protection officer (DPO) — the equivalent of a chief privacy officer (CPO) — or they are about to do so.[9] Some firms, mainly outside of Europe, are also planning to use external consultants as their DPO. But, somehow counterintuitively, the presence of a CPO doesn't necessarily mean that the GDPR budget sits with that role or that the CPO is the ultimate leader of the GDPR compliance strategy. Most often, we find the budget and the responsibility for GDPR compliance is split —

unevenly — between the DPO and a "GDPR program manager" who is usually in charge of the operational side of the program. The latter comes from the IT organization, the data governance team, or, less frequently, from other business units.

- **Firms feel prepared to tackle breach response, but they underestimate its reach.** Of the many GDPR requirements, companies are prioritizing compliance with the data breach notification requirement.[10] On the one hand, a long history of breaches and their consequences has made everyone familiar with the magnitude of the risk; hence, the will to mitigate it. On the other hand, firms are neglecting that GDPR introduces not only a duty to report the breach to Data Protection Authorities but also to the affected customers. It means that as companies get their IR capabilities ready and test them, they must also make prompt, timely, and appropriate customer communication an integral part of their incident response plan.[11]
- **There are few firms that can demonstrate privacy by design.** Examples of privacy-by-design implementation are still rare.[12] T-Systems, for instance, relies on a robust security and privacy procedure to make sure that all projects safeguard security and privacy at the core and conform to the firm's standards. ProQuest has privacy professionals as part of their scrum teams and dedicates frequent sprints to security and privacy. Even if the implementation of privacy by design might look very different from one organization to the next, embedding data privacy at the core of any initiative requires them to design and adopt processes and procedures that enable continuous collaboration across different parts of the firm, from business units to DevOps teams, from data scientists to security and privacy peers. Very often, it's about reinventing the culture of the business.[13]
- **Firms have still to figure out how to best document their compliance strategy.** GDPR compliance is not a one-off effort; firms must embed it in the way the business uses personal data daily, and it has to work as long as the firm operates. Regulators have included rules that allow them to potentially audit firms on a continuous basis. Similarly, firms must document their risk mitigation strategies on a continuous basis, too. Therefore, their approach must shift from one that is based on meeting compliance by focusing on satisfying individual requirements to one that is about building, executing, and documenting a comprehensive compliance strategy, where risks are identified and mitigated consistently and effectively.

**Recommendation**

## Build A Holistic Framework To Achieve And Sustain Compliance

When we ask firms about individual requirements, most are confident they can comply. However, implementing all the requirements and achieving the overall intent of the regulation is the real challenge. Many firms that treat GDPR requirements in isolation will find themselves in trouble. To avoid this pitfall, S&R and privacy peers must:

- **Execute GDPR programs across systems, processes, people, and governance.** GDPR compliance starts with governance. Security and privacy pros must develop a strategy with defined — and business-aligned — objectives that they want to achieve, a plan about how to achieve them operationally, decision structures to ensure allocation of accountability and responsibility for the program, and mechanisms that allow firm to measure and manage their performance. They must assess their existing processes, systems, and their people's skills against their plan, and design and implement all the necessary changes in accordance with GDPR. While we found that privacy objectives that don't align to business objectives are obstacles to the success of the program, we also witnessed cases where the GDPR initiative morphed in a broader privacy program aimed at defining the culture of the organization and its interaction with the ecosystem of its partners and customers.
- **Involve all appropriate teams from day one.** GDPR compliance is not a one-team job. Privacy by design alone suggests that continuous collaboration across teams such as application development, IT ops, and security is essential. Although the privacy or security team will most likely lead a firm's GDPR initiatives, each business unit and critical function, including customer experience (CX), human resources (HR), and procurement, will play an important role in enabling the firm to comply with the regulation. To do that, security and privacy pros must define clear rules of engagement so that each team knows the basic tasks it must accomplish. They must also guide their peers in developing an understanding of risks generated by the usage of personal data, what is aligned with the firm's policy, and what is at odds with it.
- **Invest in compliance management solutions to support continuous GDPR compliance.** While Article 30 of GDPR demands that organizations keep a record of certain processing activities, firms must also prove that they have: 1) complied with data subject rights, consent requirements; 2) run a data protection impact assessment (DPIA) when appropriate; and 3) identified and mitigated risks. Establishing the right methodology and selecting the right tools to do this is not easy. Security and privacy pros must look for automated and scalable solutions. For example, platforms that allow to feed data automatically from existing data discovery and classification tools or from data repositories are helpful. They must also choose products that allow for customized risk scoring and policies, generation of reports when necessary, and easy integration with other systems that enforce the policies.

## Supplemental Material

### Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2017 was fielded between May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Data Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Data Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

## Endnotes

[1] EU regulators will start enforcing the GDPR regulations in 2018, which means security and privacy professionals must act now to meet the deadline. For an overview of core requirements and related changes, see the Forrester report "Brief: You Need An Action Plan For The GDPR."

[2] With the deadline to become GDPR-compliant fast approaching, privacy and security professionals must act to achieve the milestones required to hit the May 2018 deadline. For more, see the Forrester report "The Five Milestones To GDPR Success."

[3] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[4] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[5] Source: Forrester Data Global Business Technographics Security Survey, 2017.

[6] For key lessons we've gleaned from financial services firms as they gear up to address GDPR compliance, see the Forrester report "Best Practices For Privacy And GDPR In Financial Services."

[7] According to our survey of security decision makers, 37% of firms in financial services and insurance say that they are fully GDPR-compliant, compared with 27% of retail and wholesale firms and 27% of media, entertainment, and leisure firms. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[8] The GDPR and update of the ePrivacy Directive will require that marketers take burdensome procedural and technical steps before collecting, processing, and using consumer data for marketing and advertising. To understand the impact, see the Forrester report "Digital Advertising Under GDPR Hinges On Data Management."

[9] According to our survey of security decision makers, 32% of firms that are not yet GDPR-compliant have hired a data protection officer and 34% are currently working on hiring one. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[10] According to our survey of security decision makers, 31% of firms that are not yet GDPR-compliant say that they are prepared for the 72-hour data breach notification requirement; 37% are currently working on it, and 22% are making plans to meet the requirement. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[11] An incident response plan is not complete unless it includes considerations for customer-facing breach notification and response. See the Forrester report "The Forrester Wave™: Customer Data Breach Notification And Response Services, Q4 2017" and see the Forrester report "Planning For Failure: How To Survive A Breach."

[12] According to our survey of security decision makers, 33% of firms that are not yet GDPR-compliant say that they have fully implemented privacy by design; 34% are currently working on it, and 24% are making plans to meet the requirement. Source: Forrester Data Global Business Technographics Security Survey, 2017.

[13] Privacy pros preparing to comply with the EU GDPR need to collaborate with other teams, including marketing, legal, and procurement, to support their overall compliance road map. See the Forrester report "Identify Companywide Roles And Responsibilities To Support Your GDPR Compliance Efforts."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

## We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

## Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

**Marketing & Strategy Professionals**

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

**Technology Management Professionals**

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

**Technology Industry Professionals**

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.


141679