The Five Milestones To GDPR Success

To Meet The May 2018 Deadline, Security And Risk Pros Must Prepare Today

by Enza Iannopollo

April 25, 2017

Why Read This Report

With the deadline to become GDPR-compliant fast approaching, privacy and security professionals must act now. However, the task feels overwhelming. Where should I start? What should I include as part of my strategy? Is there anything that I am forgetting? This report helps privacy and security professionals answer these questions and lays out the key milestones they must achieve to hit the May 2018 GDPR deadline.

Key Takeaways

GDPR Success Requires Companies To Achieve Five Milestones

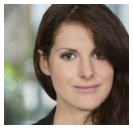
Organizations worried about GDPR requirements must take a systematic approach that begins with a maturity assessment and gap analysis, encompasses testing, and includes ongoing processes for continued improvement.

Long-Term Success Requires Risk-Management Discipline

Privacy and security pros are right to tackle GDPR as a discipline of risk management. To determine which risks they need to address most urgently, they must balance privacy risks with high-value business initiatives.

The Five Milestones To GDPR Success

To Meet The May 2018 Deadline, Security And Risk Pros Must Prepare Today



by Enza Iannopollo
with Stephanie Balaouras, Bill Barringham, and Peter Harrison
April 25, 2017

Table Of Contents

Related Research Documents

Assess Your Data Privacy Practices With The Forrester Privacy And GDPR Maturity Model

Best Practices For Privacy And GDPR In Financial Services

Brief: You Need An Action Plan For The GDPR

FORRESTER®

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

Start Preparing For The GDPR Deadline Before It's Too Late

Shockingly, half of organizations across the EU and the US are unaware of the new European General Data Protection Regulation (GDPR). Even more worrisome, the rate of awareness is lowest among tech companies.[1] But data protection authorities across the EU are gearing up the implementation of the new rules — which include fines up to 4% of global revenues for violations.[2] All firms providing services or products to European markets and/or those collecting data from European residents must prepare now. We have identified five milestones to help organizations develop and execute their GDPR strategies (see Figure 1).

FIGURE 1 Firms Must Reach Five Milestones For GDPR Success

Milestone	Action	Complete
Assessment and gap analysis	• Discover and classify data. • Map data flow. • Analyze gaps.	
The business case	• Quantify resources for hiring/training people. • Estimate costs for new products and services. • Account for professional services.	
Detailed road map to address gaps and new requirements	• Deploy security controls. • Update processes. • Mitigate third-party risks. • Review privacy notices and communication. • Define organizational design.	
Incident response testing, auditing, and process evaluation	• Test the incident response plan. • Audit your audit mechanisms. • Try out new processes. • Evaluate all customer-facing materials.	
Feedback loop for ongoing compliance and improvement	• Prepare for ad hoc audits. • Establish training and awareness programs. • Measure.	

Milestone 1: An Assessment And Gap Analysis Of Your Current Privacy Maturity

This milestone helps privacy and security pros determine the maturity of their privacy practices today. Forrester's Privacy And GDPR Maturity Model provides a comprehensive maturity assessment that goes beyond the core requirements of the GDPR to include the capabilities necessary to use privacy as a competitive advantage. In order to reach this milestone, at a minimum, privacy and security pros must:

- **Conduct data discovery and classification exercises.** To protect data, you need to know where it is and determine its risk profile. It's easier said than done, as our research reveals that a large number of companies still struggle to gain visibility into their data assets.[3] However, our data also shows that the adoption of data classification solutions is on the rise.[4] Privacy and security pros must enact processes to enable their firms to dynamically and continually classify data.[5] Sensitive personal or customer data stored and/or processed in the cloud has a higher risk profile.
- **Map data flow.** When establishing data risk profiles, privacy and security pros must consider not only where data resides in a moment in time but also how it moves across the organization and its partners. Privacy and security teams must pay particular attention to third parties. In fact, the GDPR makes third-party risk even greater. For example, while data processors will be jointly responsible for privacy incidents, businesses will have the responsibility to perform and document recurring audits of third parties' security and privacy practices and infrastructure.
- **Find the gaps in their processes, systems, oversight mechanisms, and skills.** Once you have gained visibility into data and its flow and assessed its risk profile, you are ready to evaluate current risk-mitigation strategies. This includes, for example, reviewing the implementation of security controls. Privacy and security pros must look at processes, systems, oversight, and skills as part of the gap analysis, too. To identify gaps to fill, you must consider GDPR requirements and your firm's risk appetite. Some firms in financial services, for example, deploy identity and access management (IAM) policies that are more stringent than the GDPR will require.[6]

Milestone 2: A Business Case For The Appropriate Budget

Firms must use their gap analysis to estimate the appropriate budget for their GDPR program. Thus, the investment will vary by organization. However, early research suggests that US firms, for example, are allocating approximately $1 million for GDPR compliance.[7] Whatever the amount, your business case should not be focused only on GDPR fines. Instead, it must make the case for the business benefits that the organization can realize through improved customer engagement, customer experience, and loyalty, for example. When estimating the budget, privacy and security pros should also:

- **Quantify resources for hiring and training staff.** Privacy and security training is not new, but GDPR brings it renewed attention. In fact, GDPR makes it part of organizations' risk-mitigation strategies. And our data shows that internal misuse of data is still the most common cause of data breaches.[8] In addition, GDPR requires organizations to hire a privacy officer.[9] While the International Association of Privacy Professionals (IAPP) expects that firms will need 28,000 new data protection officers (DPOs) in Europe alone, people with the right skill set are scarce, and dedicated recruitment firms are popping up quickly.[10] To secure the right hire, organizations must prepare to put competitive offers forward.[11]
- **Evaluate how much new products and services will cost.** When initiating a GDPR program, going out shopping is not a good start — it's like going to the grocery store when you're already hungry. Firms must first assess existing security controls and their deployment. They must work

with (and challenge) vendors to leverage existing capabilities to meet GDPR requirements where possible. But many organizations will need to complement their tool sets. Our inquiries with user clients show that interest in technologies such as data discovery and classification, data loss prevention (DLP), encryption, IAM, and threat detection is on the rise because of GDPR programs.

› **Account for external support with the GDPR program design and implementation.** The landscape of privacy and GDPR professional services is growing quickly. Forrester has analyzed the offerings of major consulting services companies and law firms in the past.[12] Security vendors and IT service providers are also creating GDPR consulting offerings to sell separately from their product offerings. The data breach notification requirement alone is driving organizations to consider whether to engage players such as cyberinsurers, forensics and incident response (IR) providers, and breach notification providers, among others.[13] But whether or not a firm needs professional help, privacy and security pros must define the scope of the project carefully before engaging service providers. The scope analysis will also help organizations decide which type of services they need and what vendors are best suited for the job.

Milestone 3: A Detailed Road Map To Address Gaps And New Requirements

This milestone is all about taking action, and the goal is to implement the changes that organizations identified at milestone 1. Privacy and security pros must approach this task by creating a process to assess risks systematically. This will help firms understand priorities, critical pain points, and areas for improvement. To reach milestone 3, privacy and security pros must:

› **Deploy security controls in line with GDPR.** The precision of the deployment of security controls matters. Thus, privacy and security pros must make sure that they deploy new and existing solutions to meet specific GDPR requirements. For example, they should manage identity and access in a way that is consistent with specific purpose-limitation policies. They should also prefer DLP solutions that allow for systematic reporting. When deploying encryption, privacy and security teams must pay attention to how they manage encryption keys. Not all organizations can handle keys on-premises, but they all must make sure to retain sole control of the keys and comply with data residency requirements where appropriate.

› **Update processes.** Organizations must set up new processes and redesign some old ones. Requirements such as Privacy by Design are all about processes. In fact, firms must have processes that allow peers from business units, products, data, security, and privacy to work in a collaborative manner throughout the life cycle of a new product or service. But, first and foremost, businesses must enact a process to risk-assess every data-driven initiative. Those that present higher risk must undergo a proper privacy impact assessment (PIA), and in some cases, firms must share them with regulators. Managing customer consent as well as addressing customer requests such as data portability or data deletion also requires more efficient processes.

- **Mitigate third-party risks.** Managing third-party risk is crucial to protect businesses' reputations and customer engagement — and GDPR brings new emphasis to this area.[14] For example, while GDPR requires joint responsibility for data processors — companies that handle customer or employee personal data on your behalf — in the event of a breach, it demands that firms perform meaningful audits on their third parties. Privacy and security pros must work with procurement, vendor management, and auditing peers to select third parties that comply with business privacy requirements and audit them systematically. Privacy pros at a European bank, for example, set up metrics and service-level agreements (SLAs) to determine whether third parties meet privacy requirements over time and flag issues to their colleagues in auditing as needed.
- **Review privacy notices and communication.** Organizations don't often recognize that customer-facing communication impacts the overall customer experience. In the next 13 months, virtually all firms must review this material to ensure that it reflects GDPR requirements.[15] This includes, for example, reworking all language you use to gather customer consent and for third-party data sharing. In doing so, privacy and security pros should leverage customer journey maps to identify all customer-facing communication, redesign it in line with the new requirements, and ensure that the language, the detail of the information, and the time when the communications are displayed deliver a good customer experience.
- **Define organizational design.** While many organizations must hire a data privacy officer, the GDPR does not include rules around the privacy team. However, firms will find this appropriate. Privacy teams vary in size, tasks, and reporting structures. Our research highlights four types of privacy organizations.[16] When deciding on team design and responsibilities, firms must consider industry-specific requirements as well as the goals that the team should accomplish. For example, highly regulated industries, such as financial services, have traditionally tasked their legal counsel with data privacy responsibilities. Today, many of these firms plan to establish a privacy team to promote more collaboration with other business units and help them leverage data assets more strategically.

Milestone 4: A Comprehensive Plan For IR Testing, Audit, And Process Evaluation

No one wants regulators, or, even worse, their customers, to realize that something is not working as planned, especially when it comes to data privacy. Therefore, privacy and security pros must make sure to test and evaluate whether the changes that they've implemented deliver as expected. To reach this milestone as a privacy and security pro, you must:

- **Test your incident response plan.** You don't have an IR plan if you don't test it.[17] A data breach represents a challenging event in the life of a business, and the GDPR breach notification requirement makes it even more difficult. But if you handle it properly, a breach could become a constructive event. It all depends on how well organizations plan — and rehearse — for failure.[18] Beyond the usual suspects, such as the operations team, the security team, and dedicated privacy folks, an IR plan must also include business executives, customer experience and marketing peers,

external stakeholders such as PR and communication firms, and cyberinsurers, if necessary.[19] This extended team must prepare and test the way — and the information — it would share not only with regulators, but with its customers, too.

- **Audit your audit mechanisms.** Reviewing audit mechanisms is extremely important for two reasons. First, GDPR has a specific requirement for firms to document compliance strategies continuously. Regulators can ask to review this documentation in the absence of a privacy incident or customer complaint. Therefore, it's crucial that auditing mechanisms provide firms with this evidence. At this stage, privacy and security folks must also determine whether security controls are reducing risks at an acceptable level. Second, they should pay attention to third-party audits and evaluate whether they need to complement periodic audits of third parties' infrastructure security and privacy practices with independent reviews or self-assessments.
- **Try out new processes.** Among all new processes to test, it's a good idea to start with the ones that enable the organization to comply with data subject requests. These processes must accomplish their purpose in a timely and cost-effective manner. It took one company 30 hours' worth of work to respond to a data portability request. Privacy and security pros must also verify that they can ensure these requests include data shared with third parties. Finally, they must consider whether their current technology will allow them to search and segment data in a quick and effective manner. This includes emails, archives, and backups.
- **Evaluate all customer-facing materials.** Privacy and security teams must put themselves in their customers' shoes and evaluate their customer-facing privacy communication. This exercise helps them understand if the communication is clear, transparent, and written in plain language. Make sure that consent is easy to identify and requires the customer to actively demonstrate her will to opt in. Opt-out options must be meaningful. Finally, privacy and security teams must ensure that the communication, language, and design deliver a satisfying customer experience overall.[20]

Milestone 5: A Continuous Feedback Loop For Ongoing Compliance And Improvement

GDPR is about ongoing compliance. Firms that approach this task as a one-off effort will face the risk of failure. Therefore, privacy and security pros must make sure to continuously monitor, adjust, and document their compliance strategies. To reach this milestone, privacy and security pros must:

- **Prepare for ad hoc audits.** The GDPR empowers regulators to audit firms at any time. In fact, it requires organizations to document their compliance strategies on an ongoing basis. Data shows that privacy teams in many organizations are working to set up privacy accountability frameworks to help them with this task.[21] But privacy and security pros must also leverage reporting and visualization capabilities embedded in security technologies they're currently using whenever possible. These include IAM and threat detection solutions, for example. They must perform and document risk assessment and PIA analysis continuously.

› **Establish training and awareness programs.** A recent study of privacy professionals showed that firms have increased their investments in training and awareness programs. Almost 60% of companies in the UK are investing in privacy training for staff and employees.[22] GDPR defines awareness and training as fundamental for effectively mitigating risks. Traditionally, privacy and security teams have struggled to succeed in engaging peers with training and awareness. But today, privacy has become a business topic, and large data breaches have generated a great deal of attention. Privacy and security teams must get creative and leverage this renewed focus on the topic through the right mixture of classical training, videos, podcasts, blogs, and other visual media to engage their audience.

› **Measure.** Privacy and security teams must set metrics that help track the achievements of their data privacy and security programs. Traditionally, these metrics cover operational effectiveness and compliance; for example, number of investigations. But privacy and security teams must develop their approaches to align data privacy metrics to business objectives. For example, the number of customer opt-ins or the number of initiatives that the privacy team leads jointly with the marketing team are potential metrics to consider.[23]

Recommendations

Make Risk Assessment Your Key To Success

The GDPR is all about mitigating the risks of privacy incidents effectively. To comply with the GDPR, privacy and security pros must create and leverage risk assessment frameworks to:

› **Prioritize.** Without a disciplined approach, GDPR will be an overwhelming task for many organizations. Privacy and security folks must balance privacy risks with the values of business strategies and the underpinning operations. To prioritize their initiatives, they must focus on high-risk and high-value areas.

› **Ensure executives define the overall risk appetite of the firm.** Financial services firms deal with risk-based decisions daily. In those firms, risk usually belongs to a business owner. Typically, business executives determine the risk appetite of the business overall. As part of their risk assessment frameworks, privacy and security professionals must set up processes to determine who owns specific risks and define the escalation procedures when risks trump the business risk appetite.

› **Establish a risk culture across the organization.** Culture is arguably the biggest challenge for firms on their way to GDPR compliance.[24] More precisely, in organizations that understand privacy only as mere compliance, it's the necessary culture shift that concerns privacy and security professionals. As they work to establish a corporate culture for privacy, they must also include education about risk management and risk appetite in their efforts.

Supplemental Material

Survey Methodology

The Forrester Data Global Business Technographics® Security Survey, 2016, was fielded in March through May 2016. This online survey included 3,588 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's 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.

Endnotes

[1] Source: "Preparing for the EU General Data Protection Regulation," International Association of Privacy Professionals (IAPP) (https://iapp.org/media/pdf/resource_center/TRUSTe_GDPR_Report_FINAL.pdf).

[2] Source: Dr. Kuan Hon, "GDPR: potential fines for data security breaches more severe for data controllers than processors, says expert," Out-Law.com, May 10, 2016 (http://www.out-law.com/en/articles/2016/may/gdpr-potential-fines-for-data-security-breaches-more-severe-for-data-controllers-than-processors-says-expert/).

[3] See the Forrester report "Rethinking Data Discovery And Data Classification Strategies."

[4] See the Forrester report "Market Overview: Data Classification For Security And Privacy."

[5] See the Forrester report "Rethinking Data Discovery And Data Classification Strategies."

[6] See the Forrester report "Best Practices For Privacy And GDPR In Financial Services."

[7] See the Forrester report "Assess Your Data Privacy Practices With The Forrester Privacy And GDPR Maturity Model."

[8] Source: Forrester Data Global Business Technographics Security Survey, 2016.

[9] See the Forrester report "Brief: You Need An Action Plan For The GDPR."

[10] Source: DPO Network Europe (http://www.dponetwork.eu/) and Data Protection and Privacy Recruitment (http://www.godpo.eu/).

[11] Source: Joon Ian Wong, "Privacy fans, Europe has a very lucrative job for you," Quartz, April 20, 2016 (http://qz.com/665054/privacy-fans-europe-has-a-very-lucrative-job-for-you/).

[12] See the Forrester report "Vendor Landscape: Global Privacy And Data Protection Consulting Services."

[13] See the Forrester report "Vendor Landscape: Global Legal Privacy And Cybersecurity Services."

[14] See the Forrester report "Understand The Business Impact And Cost Of A Breach."

[15] Source: Jo Pedder, "ICO guidance for consent in the GDPR," Information Commissioner's Office blog, March 2, 2017 (http://iconewsblog.wordpress.com/2017/03/02/ico-guidance-for-consent-in-the-gdpr/).

[16] See the Forrester report "Build A Privacy Organization For Consumer Data Management."

[17] See the Forrester report "Planning For Failure: How To Survive A Breach."

[18] See the Forrester report "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016."

[19] See the Forrester report "Vendor Landscape: Global Legal Privacy And Cybersecurity Services."

[20] See the Forrester report "Best Practices For Privacy And GDPR In Financial Services."

[21] Source: "Privacy Pros in the Know Aren't Waiting for Brexit: They're Preparing for the GDPR," International Association of Privacy Professionals (IAPP) (https://iapp.org/media/pdf/resource_center/Brexit-Report_FINAL.pdf).

[22] Source: "Privacy Pros in the Know Aren't Waiting for Brexit: They're Preparing for the GDPR," International Association of Privacy Professionals (IAPP) (https://iapp.org/media/pdf/resource_center/Brexit-Report_FINAL.pdf).

[23] See the Forrester report "Data Privacy Metrics That Matter To The Business" and see the Forrester report "Zero Trust Security Metrics That Matter To The Business."

[24] Source: "GDPR should drive cultural change and greater accountability on data privacy, says Denham," Out-Law.com, March 6, 2017 (https://www.out-law.com/en/articles/2017/march/gdpr-should-drive-cultural-change-and-greater-accountability-on-data-privacy-says-denham/) and Courtney Allen and Chiara Rustici, "How the EU's GDPR affects all of us," O'Reilly, October 28, 2016 (https://www.oreilly.com/ideas/how-the-eus-gdpr-affects-all-of-us).

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.