Brief: You Need An Action Plan For The GDPR

The General Data Protection Regulation Will Change The Way You Do Business

by Enza Iannopollo

October 14, 2016

Why Read This Brief

The EU General Data Protection Regulation (GDPR) will go into force on May 25, 2018. Every organization — regardless of its location — doing business with EU customers will need to make changes to its oversight, technology, processes, and people to comply with the new rules. But where should you start? This report helps security and privacy professionals understand five core GDPR requirements and two related changes they need to start tackling today.

Key Takeaways

The EU GDPR Is Finally Here

EU regulators adopted the final text of the General Data Protection Regulation in May 2016. There are no more changes on the way, so you have no more reasons to delay. You should already be setting your company up for compliance by now.

Start Addressing Five Core Changes

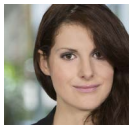
GDPR brings a variety of new rules, the most significant of which require a data protection officer (DPO), data breach notification, privacy-by-design and by-default, extraterritorial compliance, and risk management documentation, including a privacy impact assessment (PIA).

Leverage Your Efforts Beyond GDPR

Privacy Shield and the potential effects of Brexit will also affect the privacy strategies of many organizations. Identify how you can leverage GDPR efforts to meet these additional requirements.

Brief: You Need An Action Plan For The GDPR

The General Data Protection Regulation Will Change The Way You Do Business



by Enza Iannopollo
with Christopher McClean, Fatemeh Khatibloo, Bill Barringham, and Andrew Reese
October 14, 2016

It's Action Time For Your GDPR Plan

The text of the new EU General Data Protection regulation is here; no more changes are on the way.[1] Regulators will start enforcing the rules in 2018, which means security and privacy professionals must act now to meet the deadline. As you push your company's privacy strategy forward, make sure your efforts include appropriate changes to oversight, technology, process, and people.[2]

Five Core GDPR Rules Require Your Attention Now

A mature data privacy program is not built in a day. Start your action plan by assessing the core changes of the GDPR, then implement the required controls and fill any potential skill gaps. Specifically, there are five sets of changes in the GDPR that will demand significant effort for most companies:

1. **The data protection officer (DPO) will become a key security stakeholder.** The GDPR requires companies to hire a DPO if they engage in regular, systematic collection or storage of sensitive customer data. The International Association of Privacy Professionals (IAPP) estimates that the world will need almost 30,000 privacy officers to satisfy this requirement.[3] DPOs will come from inside or outside of the firm, and their backgrounds may include privacy, legal, security, marketing, or customer experience.[4] Security leaders will have to share with DPOs implementation and oversight responsibility for some security controls, such as identity and access management (IAM) and encryption.[5] DPOs will also become key influencers in the purchasing decisions about these security controls and many related business technologies such as CRM and analytics platforms.

   Action: Prepare to partner closely with the DPO to manage customer privacy. Security and privacy are interdependent, but not interchangeable. Therefore, security leaders and DPOs must work closely together to comply with GDPR and meet the privacy expectations of their customers. Many DPOs will come from the security organization, and many chief information security officers (CISOs) will wear the DPO hat themselves. But when this is not the case, security leaders must understand the background of their DPOs to collaborate and communicate with them effectively.

FORRESTER®

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

2. **The Data Breach Notification requirement will be a game-changer.** The GDPR gives companies 72 hours from the moment they become aware of them to report any data breaches to authorities and affected customers. Compliance with this requirement will be tougher than many companies expect.[6] They will first have to understand and share complicated details with regulators about any exfiltration of personal data, including how many records were lost or stolen, over what period. However, the bigger challenge is that they'll also have to share those details with customers. That means you and your incident response team will have to craft clear, compelling messages that reflect adequate levels of competency, sensitivity, and customer care.[7]

   Action: Become an incident response (IR) orchestrator. Start updating your IR plans accordingly. Prepare for the broader implications of this requirement, including its impact on customers, share value, and revenue.[8] The broad IR ecosystem includes the DPO and legal peers, as well as customer experience and marketing colleagues. You'll also need to engage with partners outside of the organization, such as law firms, regulators, PR firms, and cyberinsurance providers.[9] With so much to manage in a short period of time, you'll have to master the broker role, where your people skills will count as much as technical capabilities.

3. **Privacy-by-design will be the biggest challenge to address.** The GDPR states that firms must consider privacy at the start of any new project and ensure that the right security controls are in place throughout all development phases. Sustained collaboration between teams will be critical, so firms will have to establish new processes to encourage, enforce, and oversee it. For example, security and privacy experts should sit with the marketing team to build the business requirements and development plan for any new app to make sure it complies with the new regulation.

   Action: Improve your business skills to successfully implement privacy-by-design. Privacy-by-design is an opportunity to ingrain privacy and security in the business. But to be successful, security leaders must combine their expertise with a clear understanding of business goals, such as improving customer engagement and customer experience. These might be unfamiliar at first, but it's essential for you to identify and cover the gaps in your knowledge now or your job might be at risk.[10] You should also be able to guide business owners as they craft plans to meet privacy-by-design requirements.

4. **The extraterritorial reach of GDPR will make it a global mandate.** The GDPR also requires compliance from non-EU organizations that offer goods or services to EU residents or monitor the behavior of EU residents. Firms that already comply with existing data protection rules will need to evolve their privacy practices toward the GDPR, but a large number of firms will have to tackle privacy rules for the first time. This includes not only companies that offer products or services directly to EU residents but also those that operate as part of larger value chains. For example, a US-based data aggregator that collects and resells EU customers' data to other business partners will need to comply fully with GDPR requirements, rather than simply meeting international data transfer rules.

Action: Secure budget for GDPR compliance and third-party assessments. If you're unsure whether GDPR applies to you, it's time to bring this question to your DPO or legal counsel. If the GDPR applies (and it almost certainly does), you'll have to work on a business plan highlighting the breadth of required changes, the risks of delaying investment, and the benefits of compliance (e.g., a much larger target market). Likewise, security teams will have to engage with the procurement department to verify security and privacy controls among their third parties, starting with an assessment of their compliance status under new privacy rules.

5. **Providing evidence of risk mitigation counts as much as securing data.** According to GDPR requirements, organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Even in the absence of a privacy breach or customer complaint, regulators may require firms to exhibit evidence of their compliance and risk management strategies, including a privacy impact assessment (PIA) when appropriate. Security teams play a crucial role in building this documentation. For example, they must demonstrate that they have deployed access controls and rights management, paying special attention to processes for access recertification. Tokenization, encryption, and key management controls will require documentation, as well.

   Action: Leverage existing controls to meet GDPR requirements. Build evidence of the mitigation strategies and controls you've already deployed. Involve the DPO to help prioritize risk mitigation in accordance with the PIA. Ask security providers how to get the best evidence from their products to demonstrate compliance. For example, regulators are increasingly interested in understanding who in an organization has access to personal or sensitive data.[11] So a dashboard through which your team can easily track that will come in handy.

Consider Additional Changes As You Take Action On GDPR

The GDPR will bring many changes to your organization and your security team. However, you can't implement a compelling strategy if it undermines efforts related to other requirements. There are two recent, notable examples:

1. **Privacy Shield is the new framework for international data transfers.** After months of uncertainty, firms that transfer data from the EU to the US can now certify their practices under Privacy Shield. While the framework is based on seven principles like Safe Harbor, make no mistake: Privacy Shield is significantly different from Safe Harbor. For one, firms must provide customers with details about their privacy practices, including enforcement bodies and options for settling complaints. Other changes include a new data retention requirement and the duty to keep records of compliance with the framework. Under Privacy Shield, organizations must also update their third-party contracts to reflect new rules for data transfers.

   Action: Adopt new policies and processes for Privacy Shield. The good news is that some of the new Privacy Shield requirements align with the GDPR. For example, data retention and record-keeping requirements under Privacy Shield are similar to those in the GDPR. Work with your DPO to identify which policies and processes apply under both regulations. As the strategy matures,

you'll also have to plan for specific Privacy Shield requirements. Enforcing privacy in third-party relationships, for example, will require you to review third-party security and privacy requirements and work with peers from procurement to determine how to update existing contracts.

2. **Brexit will not dilute GDPR compliance, but data transfer agreements may suffer.** While governments around Europe work out what Brexit really means, you'll have to go ahead with your GDPR implementation. If the EU considers UK privacy standards inadequate as a result of Brexit, transferring data from other EU countries to the UK would become a more complex exercise, with implications for data transfer agreements as well as for UK-based data storage and processing activities.

   Action: Conduct a thorough risk assessment of data handling practices. Assess risks and build mitigation strategies to address different Brexit scenarios.[12]. Start from a model that considers three possible outcomes: 1) No effective changes, 2) partial changes, or 3) full Brexit. Then map the risks of your data practices for each outcome and build contingency plans accordingly. For example, in case of a full Brexit, firms that use cloud providers with UK-based data centers must consider the impact of terminating or renegotiating these contracts. Security leaders must act on five core changes in the GDPR (see Figure 1).

FIGURE 1 Security Leaders Must Act On Five Core Changes In The EU GDPR

Regulatory change	Description
Data protection officer (DPO)	Organizations that regularly and systematically monitor data subjects, or process Sensitive Personal Data on a large scale, must appoint a data protection officer.
Data breach notification	Organizations must report data breaches to the relevant authority (DPA) within 72 hours of detection of the breach. They must also inform affected customers about the incident, including details on the nature of the breach and recommendations to mitigate potential problems.
Privacy-by-design and by-default	Organizations must implement appropriate technical and organizational measures and procedures to ensure that processing safeguards the rights of the data subject (by design) and that, by default, they process only personal data that is necessary.
Territorial application	Non-EU organizations that offer goods or services to EU residents or monitor the behavior of EU residents must comply with the GDPR. Many organizations that are not subject to existing EU data protections will be subject to the GDPR, especially online businesses.
Documentation and privacy impact assessment	Organizations must demonstrate that they implemented appropriate measures with regard to the identification of the risks related to the processing; their assessment in terms of origin, nature, likelihood, and severity; and that they identified and implemented best practices to mitigate risks.
Privacy Shield	Principle-based framework that provides companies with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States. The framework replaces the Safe Harbor Agreement, and companies can self-certify from August 1, 2016.
Brexit	On June 23, 2016, the UK voted to leave the European Union. While there is uncertainty about how governments will react to the decision, it is possible that the Brexit will have a wide-ranging impact on trade pacts and regulations, including GDPR and data transfer agreements.

What It Means

Customers Demand More Than GDPR Compliance

While firms that meet GDPR requirements in a meaningful way will ultimately achieve better data privacy and security practices, their efforts to address growing customer expectations for privacy must move beyond compliance.[13] To succeed at that, the best firms will:

› **Adopt a cost-benefit-based approach to customer data.** Requirements such as privacy impact assessments, active mitigation of risks, and evidence of risk management measures will force firms to develop a disciplined approach to customer data. As a result, firms will learn to better assess

the costs and benefits of records they process, store, and protect. They will progressively focus on collecting, buying, processing, storing, and protecting only the data that offers them the most value and will kill the rest.[14]

› **Ingrain privacy into their cultural DNA.** Growing emotional distress around privacy breaches makes data protection an ethical and moral imperative.[15] Companies will increasingly follow examples such as BMW, IBM, and Nestlé to make privacy part of their corporate social responsibility (CSR) efforts. As a result, security and privacy pros will design practices that not only respond to regulatory requirements but also reflect their firm's internal standards, ethics, and public commitments.

› **Leverage privacy to drive superior customer experience.** Firms strive to make customer interactions distinct, sustainable, and engaging.[16] Those willing to establish privacy as a source of competitive differentiation will realize that customers' perceptions of privacy strongly affect the quality of customer interactions.[17] And security and privacy pros in these firms will work with marketing and customer experience teams to craft customer-facing privacy capabilities and communications that promote transparency, trust, and brand resilience.[18]

Endnotes

[1] Source: "Regulations: Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016," European Commission, May 4, 2016 (http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf).

For a summary of the GDPR, see the "Quick Take: EU Gives The General Data Protection Regulation Some Sharp Teeth" Forrester report.

[2] To assess the maturity of your organization across oversight, processes, technologies, and people, see the "The Forrester Privacy Maturity Model" Forrester report.

[3] Source: Rita Heimes and Sam Pfeifle, "Study: At least 28,000 DPOs needed to meet GDPR requirements," IAPP, April 19, 2016 (http://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/).

[4] For more details about the role of the DPO and how to successfully manage consumer data, see the "Build A Privacy Organization For Consumer Data Management" Forrester report.

[5] S&R leaders who want to build a solid data protection strategy must first work with their privacy counterparts to understand the limitations and conditions imposed by privacy regulations, industry standards, and corporate culture. Consequently, they must leverage existing security controls and policies — as well as data governance and data management — to translate privacy requirements into actionable mechanisms that, on one hand, allow customers, partners, and employees to remain in control of the personal data and which, on the other hand, enable firms to satisfy privacy requirements. For more details on how to leverage security controls for compliance purposes, see the "Defining Data Protection" Forrester report.

[6] European companies today still lag behind those in other regions in the prioritization of IR and forensics capabilities. But the GDPR will change companies' approach to IR planning, testing, and execution. In fact, the requirement to publicly report data breaches will make the impact of security and privacy breaches on business reputation and customer experience greater than ever before. For more details on the effects of data breaches on business reputation and how companies are preparing to meet GDPR's notification requirement, see the "Vendor Landscape: Global Legal Privacy And Cybersecurity Services" Forrester report.

GDPR also extends liability for privacy incidents and violation of the regulation to sub-contractors. However, the responsibility of reporting data breaches rests with the "data controller," regardless of third parties. To determine third-party responsibility and trigger liability, data controllers must include specific elements in third-party contracts, and data protection authorities must be able to review those contracts as well.

[7] For more information, see the "The Forrester Wave™: Customer Data Breach Notification And Response Services, Q3 2015" Forrester report.

[8] Source: Warwick Ashford, "Government committee calls on TalkTalk to publish breach report," TechTarget, June 20, 2016 (http://www.computerweekly.com/news/450298684/Government-committee-calls-on-TalkTalk-to-publish-breach-report).

[9] For more information, see the "Vendor Landscape: Global Legal Privacy And Cybersecurity Services" Forrester report.

[10] For more details on the skills that CISOs and their organizations need to tackle the challenges of new business requirements in the digital and customer-obsessed world, see the "Evolve To Become The CISO Of 2018 Or Face Extinction" Forrester report.

[11] Identity and access management becomes crucial to meet a number of requirements of GDPR. For more insight, see the "Defining Data Protection" Forrester report.

Identity and access management is also particularly important when staff accesses personal data of employees. For more details, see the "Employee Data Security And Privacy Matter More Than You Think" Forrester report.

[12] For more details on Brexit and how companies should prepare to face its short-term uncertainties and unintended

consequences, see the "Quick Take: UK Firms Must Drive Innovation In The Age Of The Customer, Despite Brexit" Forrester report.

[13] For more information, see the "The Future Of Data Security And Privacy: Growth And Competitive Differentiation" Forrester report and see the "Leverage Contextual Privacy To Create Better Location Engagement" Forrester report.

[14] For more information, see the "The Eight Business And Security Benefits Of Zero Trust" Forrester report.

[15] Source: Greg Palmer, "UK - Google v Vidal-Hall: A green light for compensation claims?" Linklaters, June 15, 2015 (http://www.linklaters.com/Insights/Publication1403Newsletter/TMT-News-June-2015/Pages/UK-Google-Vidal-Hall-green-light-compensation-claims.aspx).

[16] Customer interactions are shaped by a complex set of interdependencies that Forrester calls the customer experience (CX) ecosystem. In order to make significant and long-lasting CX improvements, companies first need to fully understand how their CX ecosystems function. To do this, Forrester recommends a process called ecosystem mapping that can systematically assess and document an ecosystem's hidden dynamics and help plan future improvements. See the "How To Map Your Customer Experience Ecosystem" Forrester report.

[17] See the "Data Privacy Metrics That Matter To The Business" Forrester report.

[18] Protecting hard-earned corporate reputations takes on greater importance as companies shift strategic priorities to win, serve, and retain customers. When a crisis strikes — whether the result of executive malfeasance, a product safety recall, a security breach, or another violation of a company's brand values — the results can be disastrous. Given that, risk professionals can no longer overlook the growing value and vulnerability of corporate reputations. See the "Brand Resilience: Understanding Risk Managers' Key Role In Protecting Company Reputation" Forrester report, see the "The Mechanics Of Trust" Forrester report, and see the "Data Privacy Metrics That Matter To The Business" Forrester report.

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.