FORRESTER®

FOR SECURITY & RISK PROFESSIONALS

Identify Companywide Roles And Responsibilities To Support Your GDPR Compliance Efforts

Many Teams Contribute To The Success Of Your Privacy And GDPR Strategy

by Enza Iannopollo
June 20, 2017

Why Read This Report

Privacy and security professionals preparing to comply with the European Union's General Data Protection Regulation (GDPR), by May 2018, need the support of their peers across the organization. This report helps S&R and privacy pros collaborate with other teams, including marketing, legal, and procurement, to support their overall compliance road map. It also helps these teams decide how to allocate tasks and enable the organization to deliver on their strategy.

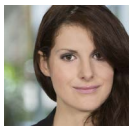
Key Takeaways

GDPR Takes A Village
Compliance with GDPR is not the result of the effort of a single team. Instead, it requires ongoing collaboration across the organization.

The Entire Firm Must Implement Basic Data Protection Skills
To achieve and sustain meaningful GDPR compliance, each business unit that handles personal data must learn the basics of data classification and risk assessment.

Identify Companywide Roles And Responsibilities To Support Your GDPR Compliance Efforts

Many Teams Contribute To The Success Of Your Privacy And GDPR Strategy



by Enza Iannopollo
with Stephanie Balaouras, Bill Barringham, and Peggy Dostie
June 20, 2017

GDPR Compliance Takes A Companywide Strategy

Collaboration across the organization is essential to meet the upcoming GDPR requirements.[1] Although the privacy or security team will most likely lead a firm's GDPR initiatives, each business unit, including customer experience (CX), human resources (HR), and procurement, will play an important role in enabling their firm to comply with the regulation. And effective collaboration requires clear rules of engagement so that each team knows the basic tasks it must accomplish.

Each Business Unit Must Address Its Core GDPR Responsibilities

For many organizations, GDPR is synonymous with extensive change. Compliance will require a major cultural transformation, particularly for organizations that believe protecting customer data is the exclusive responsibility of the security or legal team. While security and privacy pros will lead their firm's GDPR strategy, many business units have a relevant role to play (see Figure 1).

- **The privacy team leads the strategy.** Our work with clients reveals that myriad GDPR initiatives often take place across the firm. The privacy team must harmonize all these efforts and consolidate the firm's GDPR strategy. It owns the project and is in charge of specific initiatives like gap analysis and prioritization. It must provide guidance on GDPR requirements and help other teams translate these requirements into operations and processes. Many privacy teams start from incident response planning, testing, and notification.[2] Others use privacy by design as a primer. The privacy team is also responsible for gathering and documenting evidence of the firm's compliance strategy.
- **The S&R team is the privacy team's partner in crime.** The S&R team partners with the privacy team to set up and enforce GDPR strategies by deploying security controls, such as data loss prevention (DLP), and managing foundational processes, such as data classification. S&R's contribution is essential if you are to fulfill customer requests like the right to be forgotten and data portability.[3] The team also helps data protection officers monitor and document compliance

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

© 2017 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

activities by leveraging solutions like encryption or identity and access management (IAM).[4] Too many companies still fall down on the security fundamentals, and regulators keep fining them.[5] But GDPR makes the cost of failure far greater than it has ever been, so S&R teams must seize this golden opportunity to deploy basic security measures that are still missing.

- **Business teams must master risk-based discipline for data-driven initiatives.** Business units like marketing and digital teams handle a great deal of customer data. Their S&R and privacy peers might not be aware of what data they use, who has provided it, which vendors they engage with to process/enrich it, and which (increasingly cloud-based) solutions they use.[6] At a minimum, marketing and other business teams must help their privacy peers identify their data assets, data processing activities, technologies, and any third parties that use the data. Finally, business units must help S&R and privacy teams classify data, assess related risks, identify risk owners, and mitigate related risks.
- **The CX team incorporates privacy into the customer journey.** Like the other business units, CX pros must help their security and privacy peers with data classification, risk assessment, risk ownership, and mitigation exercises. But they must also help design all customer-facing notices and communication. Privacy has a huge impact on the customer experience; done well, privacy policies can be a powerful engagement tool.[7] Privacy peers must work with their CX colleagues to ensure that the language, timing, and context of privacy notices are appropriate. They must leverage customer journeys to uncover privacy touchpoints and determine the sequence and depth of privacy notices and layered privacy policies.
- **HR leads employee-data compliance efforts.** The GDPR also changes the way organizations handle employee data.[8] HR teams must approach GDPR from a starting point of gaining consent for data processing. As the employer is in a position of power, it should not rely on consent by default but should opt for legitimate interest or an alternative basis when appropriate.[9] HR peers must assess when it makes sense to rely on consent by examining the following questions: “Is there a meaningful opt-out option?” and “Is it possible to stop processing the specific data if the employee withdraws consent?” Third-party data-sharing practices and their underlying contracts will be the next items on HR’s to-do list.
- **The CIO’s team focuses on GDPR planning and execution.**[10] To start, they must help security and privacy teams discover and classify the data that the firm handles. Certain technologies, such as cloud and analytics engines, generate risk in their own right. Some firms therefore build their risk assessment and analysis starting from the data that runs on these technologies.[11] The CIO’s team also plays a crucial role in enabling the organization to comply with data subject requests, such as data portability and the right to be forgotten, and it must participate in the design of new processes to handle these requests.[12] Similarly, it must help enforce the privacy policies that its privacy and security teams have set.

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Vendor management/procurement teams must help mitigate greater risks.** GDPR increases third-party risk.[13] While the new rules introduce joint responsibility between an organization and a third party, such as a provider of cloud-hosted services, it also significantly expands the responsibility of the controller — the organization buying cloud services, for example.[14] Vendor management teams must design new processes to get visibility into and document third-party data handling practices and security measures on an ongoing basis.[15] They must include new GDPR requirements in third-party contracts and align them with the organization's privacy practices.[16] And procurement teams must work with audit and compliance teams to ensure third parties observe these new requirements.
- **Legal teams support their privacy peers in making the organization comply.** Together with the core privacy team, legal teams play a crucial role in documenting their firm's compliance strategy and liaising with the regulators as necessary. They must also take the lead on tasks that require expert legal knowledge. Third-party contracts look different under GDPR, and the team must work with procurement teams to fix these. Legal teams at many organizations start by revising third-party contracts that involve transferring data internationally.[17] Employment contracts need to change as well, so the legal team must partner with HR to get them right. Finally, they must update all customer-facing material to include relevant changes, working with the CX team to craft appropriate messages.

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

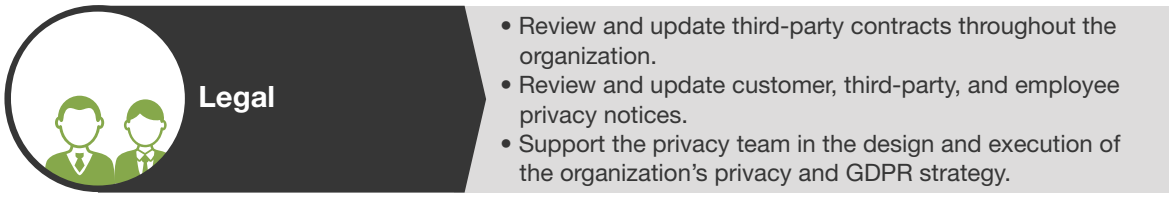
FIGURE 1 Each Team Must Tackle Three Key Areas To Enable GDPR Compliance

GDPR roles and responsibilities

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 Each Team Must Tackle Three Key Areas To Enable GDPR Compliance (Cont.)

GDPR roles and responsibilities



Recommendations

Set The Stage Before You Start The Play

Before kicking off their GDPR compliance and privacy strategy, privacy and security professionals must take care of three key points that will directly affect the result of their efforts.

› **Push privacy and GDPR to the top of your organization's priority list.** Look beyond GDPR and learn from your business leaders what role privacy plays within their broader business strategies and about the business' commitment to privacy. First and foremost, put your leaders in a position to answer these questions. Don't be shy! Bring privacy into board meetings and engage executives on the business value that privacy can deliver. Use business cases, case studies, and the results of benchmarking exercises to help shift executives' views from minimum levels of compliance to more detailed strategies on leveraging privacy as a driver of competitive differentiation.

› **Build teams that are externally oriented (your X-teams).** It's vital that you understand who will be part of the core team leading your privacy and GDPR strategy. Some organizations will build new privacy teams to respond to growing regulator and customer demands; many others will use existing structures. Either way, look to X-teams to structure your organization: X-teams are flexible, outward-looking teams that excel in their ability to lobby for resources, collaborate with other parts of the organization, and exploit connections with people and institutions outside their firm — and they perform better than traditional teams.[18]

› **Expand your vision of what's possible with privacy.** Successful X-teams look beyond their firm to gather the right information to better position, develop, and exploit their initiatives. If you're dealing with privacy, you must do this. Customer attitudes on privacy are changing rapidly.[19] If you think of privacy purely as a way to mitigate the negatives, you're missing the big picture — and a big opportunity. Leverage your external networks, benchmark your firm, enable external partners to challenge your privacy vision, and adapt your initiatives accordingly.

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Endnotes

[1] 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. To read more, see the Forrester report "Brief: You Need An Action Plan For The GDPR."

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

[3] See the Forrester report "Quick Take: EU Gives The General Data Protection Regulation Some Sharp Teeth."

[4] See the Forrester report "Defining Data Protection."

[5] Source: "TalkTalk gets record £400,000 fine for failing to prevent October 2015 attack," Information Commissioner's Office press release, October 5, 2016 (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/). Also, see the Forrester report "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016."

[6] See the Forrester report "Q&A: What Global Marketers Need To Know About European Privacy Laws."

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

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

[8] Source: "Mondaq All Regions: Employment and HR," Mondaq (http://www.mondaq.com/default.asp?product_id=0&topic_id=5); "Mondaq All Regions: Privacy," Mondaq (http://www.mondaq.com/default.asp?product_id=0&topic_id=26); and see the Forrester report "Employee Data Security And Privacy Matter More Than You Think."

[9] Source: "GDPR consent guidance," Information Commissioner's Office, March 31, 2017 (https://ico.org.uk/about-the-ico/consultations/gdpr-consent-guidance/).

[10] See the Forrester report "Customer Privacy Is A European CIO Priority" and see the Forrester report "CIOs: Find The Right Partners To Manage The Business Impact Of Data Protection."

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

[12] Source: Constantine Karbaliotis, "The Nightmare Letter: A Subject Access Request under GDPR," LinkedIn, March 9, 2017 (https://www.linkedin.com/pulse/nightmare-letter-subject-access-request-under-gdpr-karbaliotis).

[13] "In fact, the GDPR guidance suggests that the controller should also consider carrying out a data protection impact assessment prior to selecting a processor. The guidance suggests that such an assessment is prudent in all cases, but is particularly vital when the parties are handling sensitive personal data. The controller ignores at its peril signs that using a particular processor may involve high risk to personal data. The best approach if the controller wishes to proceed with that processor is to consult the relevant data protection authority first." Source: Anna Myers, "Top 10 operational impacts of the GDPR: Part 7 - Vendor Management," IAPP, February 4, 2016 (https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/).

[14] "While the controller is the entity that makes decisions about processing activities, the processor is any entity contracted by the controller for carrying out the processing. If a processor acts as a controller or outside the scope of authority granted by a controller, however, then the Regulation treats the processor as a controller for the relevant processing and it becomes subject to the provisions regarding controllers." Source: Anna Myers, "Top 10 operational impacts of the GDPR: Part 7 - Vendor Management," IAPP, February 4, 2016 (https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/) and see the Forrester report "The Five Milestones To GDPR Success."

[15] "While the Regulation imposes these heightened requirements on controllers, it is important to note that it also relaxes one of the requirements that existed under the Directive. Controllers will no longer be required to register their processing activities with a data protection authority (DPA) in each member state. Instead, the GDPR imposes strict requirements on controllers to maintain their own detailed records of processing." Source: Anna Myers, "Top 10 operational impacts of the GDPR: Part 7 - Vendor Management," IAPP, February 4, 2016 (https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/).

[16] "These provisions include how and when data will be returned or deleted after processing and the details of the processing, such as subject matter, duration, nature, purpose, type of data, and categories of data subjects. The controller and processor may also choose to use standard contractual clauses adopted by the Commission." Source: Anna Myers, "Top 10 operational impacts of the GDPR: Part 7 - Vendor Management," IAPP, February 4, 2016 (https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-7-vendor-management/).

[17] See the Forrester report "Quick Take: Goodbye Safe Harbor, Hello EU-US Privacy Shield" and see the Forrester report "Quick Take: Trust Us, We Are European."

[18] Source: Deborah Ancona, Henrik Bresman, and Katrin Kaeufer, "The Comparative Advantage of X-Teams," MITSloan Management Review, April 15, 2002 (http://sloanreview.mit.edu/article/the-comparative-advantage-of-xteams/).

[19] See the Forrester report "Introducing Forrester's Consumer Privacy Segmentation."

© 2017 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

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.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.

138191