DATUM

What U.S. Companies Really Need to Know about GDPR Compliance

FEATURING RESEARCH FROM FORRESTER

Enhance Your Data Governance To Meet New Privacy Mandates

You know GDPR is coming. You know you have to comply. But you haven't gotten your plan off the ground. Does this sound like you?

THE TOP REASON COMPANIES AREN'T READY FOR GDPR

A simple web search will yield pages of statistics on the immature state of GDPR compliance in U.S. companies. Thought provoking statistics such as:

- 50% of C level executives say that GDPR is a top priority and 75% have budgeted $1 Million or more for readiness
- By the end of 2018, over 50% of companies affected by the GDPR will not be in full compliance with its requirements.

These statistics begin to paint a picture of the state of GDPR readiness in the US. They tell us that today's companies are aware of the regulation and have even started the budgeting process, but won't have their plan in place in time to meet the deadline. So why are companies just scratching the surface on GDPR despite the looming deadline and significant penalties? **Our customers frequently cite the lack of data governance as the biggest challenge impeding readiness.**

OVERCOMING THE DATA GOVERNANCE CHALLENGE FOR GDPR

To overcome the data governance challenge, companies must have clear insight into the data that falls under this regulation: how is it coming into the organization; what happens to it while it is in your control; and what controls exist for it leaving the organization? Successful organizations will architect capabilities that not only manage the lineage of these data assets, but also actively assess vulnerabilities and risk mitigation activities.

The governance capabilities required by those leading the initiative, such as the Data Protection Officer (DPO), to monitor, enforce and report on compliance will be critical. Proving due diligence will require DPOs to establish clear linkages among policies and standards, the underlying data, and the associated use of that data across the various business processes within an organization. DPOs will need to establish metrics and measures that are both transparent and defensible to the regulatory agencies.

Learn more about the data governance capabilities that are necessary for GDPR compliance in Forrester's report below:

IN THIS DOCUMENT

Enhance Your Data Governance To Meet New Privacy Mandates

The EU's GDPR Will Require Firms To Be More Transparent With Their Customers' Data

by Henry Peyret

March 28, 2017 | Updated: April 4, 2017

Why Read This Report

Data governance traditionally addresses privacy simply by classifying data for masking or anonymization. But the EU's General Data Protection Regulation (GDPR) will change that. It introduces new consumer rights, requires the involvement of stakeholders beyond legal and security teams, and creates new responsibilities (and new fines). This means firms can no longer manually manage their customers' data privacy. This report explains how enterprise architecture (EA) pros can add privacy management and benefit from impact analysis and soft collaboration among stakeholders.

Key Takeaways

The GDPR Brings New Complexities To Privacy Management

The privacy regulation, which will go into effect in May 2018, creates new rights for consumers and new obligations for companies. For example, it will require companies to involve more stakeholders, including consumers. These additional complexities mean enterprise architects must enable a state-of-the-art privacy management practice.

Enhance Your Data Governance With Privacy Management

Data governance helps firms manage privacy without seeing costs explode due to increasing complexity. Even if you aren't affected by the GDPR or are a B2B firm, privacy must be your concern.

Data Governance Stewardship Tooling Is In Transition

Expect to see data governance stewardship and discovery tooling broadly participate to centralize the increasing complexity of privacy management. This isn't the whole solution to the GDPR, but it should greatly help.

Enhance Your Data Governance To Meet New Privacy Mandates

The EU's GDPR Will Require Firms To Be More Transparent With Their Customers' Data

by Henry Peyret
with Alex Cullen, Cheryl McKinnon, Jennifer Belissent, Ph.D., Enza Iannopollo, Alex Kramer, and Diane Lynch

March 28, 2017 | Updated: April 4, 2017

Table Of Contents

Related Research Documents

FORRESTER®

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

FORRESTER®

The GDPR Brings New Rights To Consumers And Challenges To Firms

Starting in May 2018, every company that deals with European customers must comply with the GDPR or face hefty penalties.[1] That's a broad category: Firms that are based in the EU, have EU operations, or offer products or services to EU customers are starting to determine how the GDPR will affect them. For example, a 2017 survey from Forrester and ARMA International reveals that 25% of firms have verified that the GDPR applies to them and that they're preparing to take or are taking action; 34% have verified that they're not affected; and the rest (41%) either don't know or aren't certain.[2] What should EA pros know about how the new regulation will affect their firms?

- **The GDPR introduces new customer data rights.** The GDPR provides EU consumers with four key rights: a right to access (the ability to view what data an organization has collected from them); a right to amend (if a customer finds incorrect information); a right to be forgotten (asking a company to erase all of one's data); and a right to data portability (also called "package and deliver"). This last right is one of the most complex. It allows customers to ask a firm to return any data they have directly provided the firm and also any data the firm has collected from them — including consumption data.[3] The EU's goal is to boost competition among service providers, enabling customers to move from one provider to another and give that competitor enough historical information to get the best quote or service. The right of portability will require interpretation of what defines personal customer data and which data is protected because it's the consumer's intellectual property (IP).
- **Your company's obligations differ based on the type of data you collect.** The regulation defines several types of data: data collected directly from customers (e.g., name and address); data collected automatically and obtained with consent (e.g., geolocalization data); data collected automatically without consent (e.g., phone number and call duration); computed data (e.g., credit score); and computed data using a firm's IP (e.g., customer churn or risk score). These are stored in structured databases, but there's also unstructured personal data stored in documents. Under the GDPR, companies' obligations will vary based on the type of data they collect. For example, the right to access touches a reduced view of data (e.g., name and address) compared with the right to data portability, which gives consumers rights to more data, including some that is collected automatically (but not data that is computed and protected under IP).
- **The GDPR's rules are evolving and are open to interpretation.** Despite the GDPR's attempts to harmonize data protection rules across European member states, enforcement of these rules might vary. For example, French law protects national government agencies against a customer's right to data portability. The GDPR, backed by the guidance of the Article 29 Working Party, excludes data that is protected by IP, but how far does IP extend? Guidance will continue to evolve about other types of data. For example, the European Commission is preparing a new regulation specifically for the internet of things (IoT) and machine data that could address privacy for this data.

- **Governing privacy across data ecosystem requires centralization.** Omnichannel strategies, combined with external data sources, are multiplying the instances when firms must gather customer consent. But firms shouldn't ask for consent at every channel touchpoint. As data commercialization becomes more prevalent, the sources of data will multiply, and managing obligations like "consent" and "data protection by design" across data providers, data brokers, and data buyers will become more complex. This will require EA pros to ensure an unbroken lineage of data and define who processes and controls the data (the consumer or the company) at each stage within the data ecosystem. To manage the upcoming privacy complexities and keep costs under control, EA pros should use information architecture to complement data governance and centralize privacy policies management.
- **Your firm must demonstrate compliance and due diligence.** The GDPR places a burden on the organization to defend its actions. A company should not only demonstrate that it is compliant to the GDPR but also continuously adjust to the state of the art for its vertical industry and its inherent risks about consumers' protection.[4] Because risk is constantly evolving, you must continuously update your risk analysis. This will require explicit, transparent, and defensible approaches to risk analysis that you validate in advance through engagement with regulators. In the event of a breach of personal data, organizations must demonstrate due diligence to avoid the significant penalties that are possible under the GDPR.

ENHANCE YOUR DATA GOVERNANCE AND ARCHITECTURE TO COMPLY WITH GDPR

Security and privacy best practices suggest that companies continuously classify data and take appropriate actions based on that classification — for example, encrypting or masking the personal data of customers and employees.[5] But the GDPR will:

- **Make data governance more difficult.** The GDPR will require firms to classify personal data in multiple subcategories (e.g., shareable data, portable data, and data computed from private data but designated as IP). It will also require new applications to manage the rights of consent, access, erasure, and portability. And the law will mandate that firms audit and, on demand, provide evidence of their compliance to regulators.
- **Make it hard to manage compliance manually.** Firms are exploring new uses for data, including monetizing (i.e., packaging and selling) data, which will require transparency to the customer about these new uses and data sharing by other companies. The old way of managing privacy as a matter exclusive to data security will prove insufficient under the GDPR.[6] Navigating the GDPR's complexity will require a cross-functional effort across the organization. Firms will have to leverage existing data governance practices and tools to meet these new requirements more efficiently.

Adapt Your Data Governance In Five Areas

One issue that the GDPR has revealed is that firms have viewed privacy from a few siloed perspectives, often legal, security, sales, and marketing. But our research shows that many companies have 15 or more departments that are privacy stakeholders, each with its own viewpoint.[7] The real difficulty is coordinating these multiple viewpoints and governing complex decisions that affect both compliance and your business. And you also need to coordinate this effort with your customers, with the regulators and industry groups that are establishing best practices, and with your data supplier partners. You must build a consensus among all of these stakeholders (internal and external) across five main areas of change: communication with personal information holders; building a culture of privacy within the organization; remediation for claimants; certification and risk management of partnerships; and reporting and engagement with regulators.[8]

ADDRESS PERSONAL INFORMATION HOLDER COMMUNICATION

Typical communication with "data subjects" — that is, customers — includes obtaining their consent, notifying them of data breaches, and giving them access to data. In the following figure, we translate the requirements for the data protection officer (DPO) in terms of communication (see Figure 1).

FIGURE 1 GDPR Obligations And Data Governance Impact: Communication With Personal Information Holders

Obligation	Description	Data governance impact
Consent	Companies must obtain active consent (explicit consent for specific cases) when collecting personal data from individuals and must communicate why the information is being collected, by whom, and for how long it will be kept.	Link each piece of data to data process/service in such a manner that the consumer understands why. Link consent to each data collected; create a dashboard for the data protection officer (DPO) to demonstrate compliance. Establish regular surveys for new private data obtained without explicit consent. For private data without explicit consent, there's no need to "access" or "fix" but, perhaps, to "package and deliver." Share consent information with data buyers in data commercialization.
Data breach notification	The GDPR states that companies must notify personal information holders of a data breach that "results in a high risk to the rights and freedoms of individuals."	Estimate the impact on or risk to customers' private lives and recommend actions for them to remediate risks (e.g., change their passwords to renew their accounts). Notify customers, as well as regulators, within the 72-hour answer period.
Access	Companies must grant access to personal information to individuals upon request.	Form a collaboration process to classify data as "customer accessible" and allow customer access through GDPR lineage. Manage the retention period. Specify hiding and encryption policies.

Source: DATUM and Forrester Research

BUILD A CULTURE OF PRIVACY WITHIN YOUR ORGANIZATION

Companies have not yet figured out how to build a culture that protects their customers yet still allows them to innovate and find new business models. They must develop a culture that includes privacy risk management, not only in terms of compliance with the GDPR but also, and more importantly, to stay ahead of threats to their brand reputation (see Figure 2).

FIGURE 2 GDPR Obligations And Data Governance Impact: Building A Culture Of Privacy

Obligation	Description	Data governance impact
Organizational alignment	Companies must assign a data protection officer (DPO) with appropriate resources and authority when they engage in regular and systematic monitoring of data subjects on a large scale or where their core activities consist of processing special categories of personal data.	Implement a privacy management process. Enable privacy audits for regulators, including GDPR lineage controller and processor lineage. Publish privacy audit for data buyers.
Data protection by design	Organizations must build the concept of privacy into the fabric of their data practices and their information platform architectures. Companies must manage transparency, lawfulness, data minimization, and data quality at each stage of the data life cycle. The GDPR discusses a "code of conduct" as a mechanism for formalizing practices.	Establish data flow lineage along the data life cycle. Create dashboards for CIO, DPO, and chief data officer to demonstrate data protection (security and transparency) for private data. Provide data protection auditing guidance to diminish the costs of such audits.
Risk management	The GDPR states that organizations need to "implement technical and organizational measures to ensure a level of security appropriate to risk."	Centralize the management of private data security policies executed in many apps. Deploy these policies in the execution platforms (ECM, eCommerce, and cloud platforms). Estimate enterprise impact or risks to managing customer private data. Manage the evolution of impact assessment best practices from industry consortiums.

Source: DATUM and Forrester Research

OFFER REMEDIATION FOR CLAIMANTS

In some cases, consumers will contest the accuracy of data, dispute how a firm uses their data, or rescind permission for a firm to have that data. Data governance must support a remediation claim process that provides a risk-and-impact assessment to help the different parties agree on what qualifies as personal data and thus provide more transparency and trust (see Figure 3).

FIGURE 3 GDPR Obligations And Data Governance Impact: Remediation For Claimants

Obligation	Description	Data governance impact
Data subject requests	An individual has to be able to "rectify" incorrect data held by the organization.	Provide an interface to consumers that enables data correction. This is a collaborative process to decide which data should be classified as "rectifiable".
Right to be forgotten	An individual can ask an organization to erase all data related to the individual.	Implement a collaboration process to find private data for deletion and take appropriate action. This can also rely on private classification. The data protection officer (DPO) must have the capability to demonstrate that a firm does not rely on any private data after deletion.
Restriction quarantine	An individual has the right to object and request that the organization stop processing data when there is a dispute.	Implement a collaboration process that classifies private data as "quarantinable" upon customer request in case of a dispute. The DPO must have the capability to demonstrate that a firm does not rely on any private data in quarantine.
Data portability (package and deliver)	Individuals may request that their data be delivered in a machine-readable format.	Implement a collaboration process that classifies private data as "packageable." Applications must be able to extract, deliver, and delete this information after delivery. In the event of a dispute, the DPO must be able to justify data usage and governance. through GDPR lineage.

Source: DATUM and Forrester Research

IMPLEMENT CERTIFICATION AND RISK MANAGEMENT OF PARTNERSHIPS

Data sources are multiplying, and the flow of data is becoming more complex. Companies must hold both themselves and their partners accountable. Your defense against a privacy breach is only as strong as the weakest element in your ecosystem for sharing or exchanging data. To address this problem, the GDPR requires that data suppliers and data buyers exchange privacy audit capabilities and results (see Figure 4).

FIGURE 4 GDPR Obligations And Data Governance Impact: Certification And Risk Management Of Partnerships

Obligation	Description	Data governance impact
Duty to audit and monitor data processor compliance with the GDPR	The GDPR states that organizations must "use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this regulation."	Track external processors' private data sources and their GDPR compliance. Identify and sponsor codes of conduct by industry or consortiums to provide evidence of due diligence. Exchange GDPR personal data policies as well as more global policies (compliance and ethics) with data buyers and data brokers. Allow feedback from data buyers on personal data policies.

Source: DATUM and Forrester Research

WORK WITH REGULATORS AND INDUSTRY GROUPS

Finally, to maintain a state-of-the-art privacy management practice, companies must focus on their relationships with regulators and the industry working groups that are establishing industry best practices (see Figure 5).

FIGURE 5 GDPR Obligations And Data Governance Impact: Reporting And Engagement With Regulators

Obligation	Description	Data governance impact
GDPR reporting	The organization must have the ability to catalog all events surrounding GDPR personal data, including remediation events and their status, due diligence activities, vendor certification, and internal audits.	Track GDPR activities, the evolution of interpretations of compliance, and decisions. Undertake a GDPR audit.
Privacy impact assessment (PIA)	The organization must be in position to identify "high risk" activities and is obligated to consult with regulatory authorities for those activities.	Assess privacy risk analysis. Share privacy risk analysis with regulators and industry working groups establishing state-of-the-art privacy. Share privacy risk analysis for data buyers. Collaborate with industry and regulators, and provide statistics.

Source: DATUM and Forrester Research

Data Governance Tooling Industrializes Governance For Privacy

While a company's privacy team leads the effort of managing privacy, many other teams — including security, EA, digital, and customer experience — will enforce privacy rules and policies regarding data security access, the data life cycle, data discovery, enterprise content management (ECM) access controls, data extraction, and data commercialization.[9] These platforms execute policies and rules but rarely put in place the necessary collaboration to establish and centralize policies. As a result, firms usually fail to centrally manage privacy policies and rules using these data governance execution platforms or traditional compliance software, but it's necessary to industrialize privacy management while avoiding escalating costs. Expect data governance, stewardship, and discovery tooling to provide the level of centralization required for GDPR or, more generally, to industrialize privacy management and thus offer ways to:

- **Discover, store, and manage the continuously evolving use of personal data.** In the age of the customer, the collection of customer data will continuously evolve to enable more and more personalization. But each additional data point may be subject to new consent, access, delete, and portability rights — or not. Your data governance practice should track data and its usage continuously to alert you if you risk violating one of these new rights.
- **Manage the dynamic interpretation of privacy laws.** These offerings must also manage the customized or unique customer requirements that your execution platform must integrate. The goal of data governance stewardship is to manage the right balance between opposing objectives, such as data monetization versus customer privacy concerns. A large European telecom provider revealed to us that while establishing his new data governance group and strategy, he faced this important dilemma of how to monetize data as a telco without damaging the firm's reputation for safeguarding personal data.
- **Involve all privacy stakeholders.** Privacy processes involve a large number of roles, including sales and marketing, technology management, HR, and legal.[10] Firms must manage the collaboration by, for example, establishing a responsible, accountable, consulted, and informed (RACI) table for private data. Today, data governance, stewardship, and discovery tools try to involve all employees as data stewards.
- **Enable consumers to shape use of private data for personalization.** These tools should evolve to allow a customer to decide what data to share, depending on data usage. This will become a kind of negotiation that allows customers to determine the level of customization they would like and what data they'll agree to share with a company. And as companies begin to monetize data, the customer can decide how companies can sell their data and to whom.
- **Provide the right tooling to the data protection officer.** Data protection officers need dashboards and processes to continuously manage the evolution of increasing privacy concerns. Data governance, stewardship, and discovery tools will also be key should a firm need to prove its support of data privacy and will save money by reducing auditing time and efforts in the face of regulator demands.

› **Accelerate and enable data commercialization.** Getting the right data product at the right cost — including the right contract clauses (e.g., guaranteeing shared privacy and confidentiality and that data won't be resold to competitors) — accelerates the reuse of data governance lineage, policies, and risk analysis capabilities. Data sellers must assure buyers that they've properly governed the data's privacy, and buyers must be able to access the purchased data's context to optimize their usage of it.

Recommendations

Make DGSD A Critical Part Of Your Strategy To Comply With The GDPR

Data governance, stewardship, and discovery (DGSD) is an important element of the architecture you'll need to centralize the management of privacy policies, consumer rights, and company obligations. But vendors are still developing their capabilities to comply with the GDPR. EA pros should see DGSD as complementary to their information architecture models. Your strategy will depend on your data governance maturity.

› **Enhance your current data governance stewardship to address privacy concerns.** Don't hesitate to ask vendors and their partners to boost their skills in the new and still developing GDPR domain. We're only just starting to understand the depth and complexity of that domain, so EA tooling and DGSD vendors will continue to enhance privacy capabilities.

› **Use the GDPR as a starting point if you lack a data governance stewardship package.** The GDPR (and, more generally, privacy management) can be a good starting point to enhance your enterprise data governance, which is usually limited to data quality and master data management. EA pros must recognize the need for data governance, stewardship, and discovery that covers multiple domains of data governance. But don't overhype the ability of DGSD tools to address/comply with the GDPR, as they're still in development.

› **Recognize that privacy will be mandatory, even if the GDPR doesn't apply to you.** Forrester has developed a practice for privacy management because it's essential for companies that want to gain customers' trust and loyalty — a critical element of the customer experience in the age of the customer. So even if the GDPR doesn't directly concern you, privacy must. DGSD is an important means to industrializing the privacy domain, which, thanks to the IoT, continues to enlarge.

› **Demonstrate GDPR compliance if you want to share European customers' data.** B2B customers purchasing your data will ask you to demonstrate compliance with the GDPR, and you should provide audit results to prove this. A DGSD tool will provide the right level of capabilities at the right cost to make data monetization competitive.

What It Means

Privacy Will Be Fundamental To Consumer Trust And Engagement

Privacy and security started from the same roots but are now different disciplines. Privacy also plays a crucial role in earning customers' trust. Being compliant with the GDPR isn't the end of the story. In this evolving environment, where risk to a firm's brand reputation looms large, EA pros must see privacy management not only as a way to save costs (or fines) but rather as an opportunity to enable engagement with customers. Companies that do a good job of protecting their customers' data will build a powerful competitive differentiator in the marketplace, and their privacy strategies will help grow the business. They'll not only comply with GDPR but also develop ethical guidelines to guide their business strategy execution around privacy and personalization.

Supplemental Material

SURVEY METHODOLOGY

In the Forrester/ARMA International Records Management Online Survey, Q1 2017, Forrester conducted an online survey of 295 records management decision makers from January 2017 to March 2017. Approximately 70% of respondents were located in the US. The remaining participants were based in Canada, the UK, Europe, Asia, and Australia/New Zealand.

COMPANIES INTERVIEWED FOR THIS REPORT

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Collibra

Datum

Informatica

Mega International

Software AG

Endnotes

[1] For more details about the actions that companies should take now to prepare for GDPR requirements, see the Forrester report "Brief: You Need An Action Plan For The GDPR."

[2] In the Forrester/ARMA International Records Management Online Survey, Q1 2017, 209 respondents replied to the following question: "Is your organization concerned about the upcoming European General Data Protection Regulation?"

[3] The EU's Article 29 Data Protection Working Party recently shared new guidance on how companies should implement data portability. Source: "Guidelines on the right to data portability," European Commission, December 13, 2016 (http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf).

[4] Refer to the EU's Article 24, "Joint Controllers" and Article 25, "Representatives of controllers not established in the Union." Source: "Regulation Of The European Parliament And Of The Council," European Commission, January 10, 2017 (https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-8-F1-EN-MAIN-PART-1.PDF).

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

[6] For more details about the difference between data security, data protection, and privacy, see the Forrester report "Defining Data Protection."

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

[8] The tables in this report are inspired by this Datum GDPR white paper. Source: "The Official Guide to GDPR Compliance," Datum (http://info.datumstrategy.com/gdpr-guide-ebook-paper-privacy-compliance).

[9] For more details on organizational designs for privacy, see the Forrester report "Build A Privacy Organization For Consumer Data Management."

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

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.

DATUM helps the world's leading organizations identify, organize, and use data to solve problems and create opportunities. Information Value Management® brings context to your data by capturing business rules, standards, policies and procedures and connecting them not only to the underlying data, but also to metrics, processes, and objectives. For the CDO, CROs and DPOs, Information Value Management® delivers the governance hub that aligns business priorities with GDPR compliance requirements. You can easily map out your governance structure in a way that the enitre company understands. Learn more and request a demo: http://www.datumstrategy.com/gdpr-solution