IBM Analytics
White Paper

Planning for the General Data Protection Regulation

Protect, govern and know your data with help from IBM

IBM

Overview

Customer information can offer invaluable insights into trends, behavior and spending which can lead to more targeted marketing, better consumer offers and even new and more practical products. However, using and storing personal information can also be a big risk to organizations if not handled properly.

With this in mind, European countries have developed a plethora of data protection rules, encompassing both data privacy and data security, to combat the use of personal data without an individual's direct consent or other lawful justification. Currently these rules are not only based on the outdated 1995 Data Protection Directive (DPD), but they are also inconsistently enforced. When they are enforced, the penalties are minor in comparison with the time and expense required to comply with them.

The General Data Protection Regulation (GDPR) looks to change all of that. Published in May 2016, the GDPR is in a two-year transition period. In May 2018, it will be immediately applicable to any organization that operates in the EU market or processes the personal data of EU data subjects.

According to the GDPR:

- **Processing** consists of *any* operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means. The GDPR includes examples of this in its definition.
- **Personal data** is defined as *any* data that directly or indirectly identifies or makes identifiable a data subject, such as names, identification numbers, location data and online identifiers, whether or not that data belongs to customers, employees or others, so long as they are a natural person.

With such broad guidelines, it is difficult, if not impossible, to identify organizations that will not be impacted in some way. This scope is made even wider, up to a global level, by the

extra-territorial nature of the GDPR. For example, an organization that does not have a footprint in the EU but offers goods or services to, or monitors the behavior of, EU data subjects would be bound by the GDPR, whether or not such offerings were connected to a payment of any kind.

Replacing the national laws that now exist, the GDPR seeks to create a more harmonized, unified data protection law framework for all EU countries. Goals include:

- Reinforcing and enhancing the data protection rights of EU data subjects
- Facilitating the free flow of data by harmonizing data protection laws across the EU
- Modernizing the law in line with emerging technologies

The Article 29 Data Protection Working Party (the very regulators who will enforce the GDPR as the European Data Protection Board [EDPB]) is putting in place an action plan so that it will be ready to act effectively from the time the GDPR becomes law in May 2018.

Organizations should be preparing now as well. This means gathering the people, policy, process and technology necessary to comply with the GDPR before May 2018. Now is the time to build on your existing foundations to identify gaps and implement steps to protect, govern and know your data, as noncompliance may lead to huge fines of up to €20 million or 4 percent of total annual turnover of the preceding financial year, whichever is higher.[1]

Key GDPR duties and obligations

The goals identified previously can be distilled into five key duties and obligations for any organization that touches the data of EU data subjects:

1. **Rights of EU data subjects:** The GDPR enhances the rights of data subjects in the EU. For example, it has codified and clarified data subjects' ability to request access to and erasure of their information. In addition, organizations need to provide easier access to personal data, with clear and easily understandable information on processing. Making this information available gives data subjects insight into how their information is used.
2. **Security of personal data:** A big change here for many organizations: they will now be obligated to report data breaches to regulatory authorities within 72 hours, and in high-risk scenarios, to follow this reporting by notifying the individuals whose data may have been compromised. All data must have appropriate technical and procedural measures to ensure a level of security appropriate to the risk that it carries. Organizations have an obligation to take security measures: even if you do not have a data breach, you can still be in breach of the regulation if you do not take proactive steps.
3. **Lawfulness and consent:** Processing of personal data will be lawful only if one of the six factors the GDPR lists is in play (for example, if it is necessary for the performance of a contract or if it is required for another regulatory compliance reason or legal hold). Consent is also one of these factors, but under the GDPR, consent will become even more difficult to demonstrate. Consent has strict requirements, including the fact that it can be withdrawn at any time (at which point an organization would need to rely on one of the other factors to lawfully retain the data should it wish or need to do so).
4. **Accountability of compliance:** Organizations should expect regulators to potentially exercise their powers to access data and premises, and should more generally be able to demonstrate compliance with the GDPR principles relating to personal data. Mechanisms to assist with providing this proof—including carrying out data protection impact assessments, adhering to codes of conduct and proactively seeking certification through approved mechanisms—will be available, but have not yet been fully defined.
5. **Data protection by design and by default:** Finally, data controllers must implement technical and organizational measures demonstrating compliance with GDPR core principles, ensuring the rights of data subjects are met and that only data necessary for the specific purpose is processed. In other words, data privacy for individuals should be the default action and should be designed into all organizational and technology processes from the ground up.

Gather the people, policy, process and technology necessary to comply with the GDPR before May 2018. Now is the time to build on your existing foundations to identify gaps and implement steps to protect, govern and know your data.

Recommendations

While this paper boils down a fairly substantial regulation to five key areas, the capabilities that they demand are still considerably broad in scope. It is therefore important to have a clear and defined idea of how your organization will address all the different GDPR requirements. To this end, IBM has created a solution framework that brings together the capabilities and technologies you can use to help you take important steps toward compliance with the GDPR (Figure 1).

Figure 1 shows:

- The five key GDPR duties and obligations, sitting in context atop the policies, processes, rules, analyses and audit capabilities that will eventually need to be put in place to address these requirements.
- A data management layer that has the capability to execute policies through direct interaction with all the data sources of an organization: structured and unstructured, in the cloud

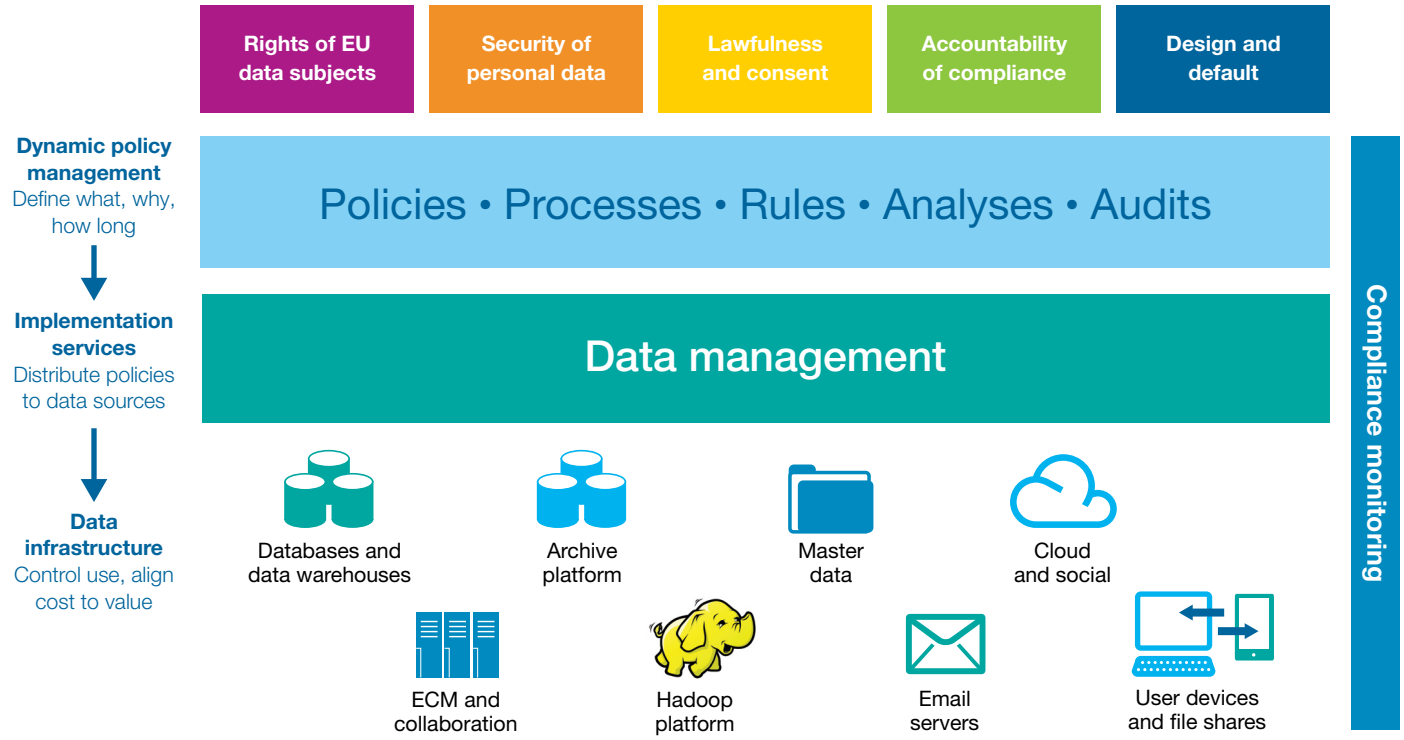

Figure 1. IBM GDPR solution framework.

and on-premises. Over time, the goal will be to automatically syndicate as many policies to the data management layer and automate as much of the policy execution as possible.
- Ongoing compliance monitoring and security event and breach monitoring.

A fundamental principle of this framework is openness and extensibility. Invariably, organizations will have made existing investments in some of the capabilities required for GDPR as part of prior data privacy and security initiatives. It's important that these investments are preserved by incorporating them into the architecture as it grows to meet the GDPR's expanded requirements.

Pragmatic steps

With this background in mind, it's time to get pragmatic. You may decide to begin by choosing a few key processes and carrying out a risk assessment. This assessment should answer the following questions:

- How likely are events that would potentially fall under the ambit of the GDPR (such as EU data subjects exercising their rights, data breaches, regulator audits and so on), and what would be the consequences if those events happen?
- What is the current state and what is the desired state?
- What people, policy, process and technology are required to get to that desired state?
- Where are the most significant technology gaps? Is the best way to close these gaps by bolstering existing investments or introducing new organizational and technology measures?

Once you start working toward your goals, make sure you track, measure and audit your improvements.

While you are working on your process, it's also a great time to perform a data assessment. The assessment should give you a good understanding of where customer data exists across your enterprise, where personal data resides, what you could potentially get rid of and where the "crown jewels" of your enterprise data live. This information can be crucial when designing processes for responding to EU data subject requests or a data breach.

Leverage the deep experience of IBM

IBM has worked with clients around the world and across many industries to help them improve both readiness and response for data privacy events. Some examples include:

- **Telecommunications:** Enhancing data privacy and security
- **Banking:** Identifying solutions that organizations can use to help address their regulatory and legal risk
- **Pharmaceutical industry:** Supporting regulatory demands and defensible disposal goals
- **Health insurance:** Assessing and securing sensitive member data

Telecommunications

A large European telecommunications company faced a problem in preparing for the new GDPR. It had little to no insight into where personal data was being stored across its enterprise or what data needed to be brought into compliance and placed under additional security.

Initially, the telecom company assessed data manually by interviewing people and studying documentation, but that process could never scale to handle the volume of data involved. The company needed a more automated approach, and one that could handle both structured and unstructured data.

The company is working with IBM to proactively locate its sensitive personal data so it can determine the best course of action to prepare for the GDPR.

Banking

A European financial services company faced significant exposures while complying with regulations such as Basel Committee on Banking Supervision (BCBS) 239, Basel II and Markets in Financial Instruments Directive (MiFID). Existing applications with limited integration and silos of data resulted in incomplete aggregation of data, delays in regulatory reporting and incorrect risk profiles.

Working with the IBM® Master Data Management (MDM) solution, the financial services firm used its data stores to create a consolidated and accurate single view of the client, enabling a real-time view of the complete customer. The solution helped the firm provide a better client experience and left it better prepared for GDPR by having the same consolidated client view irrespective of channel or contact type.

Pharmaceutical industry

A pharmaceutical company had various requirements for its data governance projects, such as establishing an efficient and appropriate approach for retaining information of business value or that was subject to regulatory requirements; preserving information needed for litigation; and thoughtfully discarding what was no longer needed.

Working with IBM, the company implemented IBM Global Retention Policy and Schedule Management to create and track policies that help the business retain, hold or dispose of data based on regulatory duty, litigation and business value. This reduced its compliance risk and allowed for routine, defensible disposal of unnecessary information.

Health insurance

A health insurance company with more than 15 million health plan members, 13 million dental plan members and 10 million pharmacy members manages, processes and is responsible for a greater amount of sensitive data than most organizations. A rapidly growing volume of patient records, emails, reports, prescriptions, insurance documents and other information needed to be properly managed and stored, with strict governance over the privacy, security and long-term archiving of patient records and other healthcare-related information.

The company wanted to find and manage personally identifiable information in its unstructured file systems as well as implement hierarchical storage management strategies across its structured data. To do this, it needed to understand where sensitive data resided and then act on that data across a vast array of data sources.

Working with IBM, the company used IBM StoredIQ® for Data Assessment to identify sensitive data in its native location and move it to more protected servers. The company was able to map its data topology showing where information resides; get an overview of storage use by department, group and even user; identify sensitive data and mask it appropriately by applying granular security; properly classify records; and appropriately dispose of unnecessary information. The health insurance organization could connect to live data sources across the enterprise, providing a consolidated view of the relevant data in minutes, not weeks.

Start planning for GDPR now with IBM

The GDPR presents a big challenge, one that organizations in many industries that conduct business globally are facing. However, the majority of the individual tenets of the GDPR are nothing new, and IBM has a long history of partnering with clients around the world to deliver enterprise-level solutions to these broad issues. Take action now to prepare your business, assess your data risks and obligations, and proactively govern your information—May 2018 is closer than you may expect.

Remember the five key GDPR duties and obligations

1. Rights of EU data subjects
2. Security of personal data
3. Lawfulness and consent
4. Accountability of compliance
5. Data protection by design and by default

For more information

To learn more about the GDPR and IBM solutions to help you protect, govern and know your data, contact your IBM representative or IBM Business Partner, or visit:

- **ibm.com**/analytics/us/en/technology/general-data-protection-regulation
- **ibm.com**/information-lifecycle-governance

IBM Analytics
Route 100
Somers, NY 10589

Produced in the United States of America
November 2016

[1] Defined under Article 83 (General conditions for imposing administrative fines), paragraph 5 and 6 of the EU GDPR. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL

Please Recycle

IMW14906-USEN-00