OPERATIONALIZE YOUR ORGANIZATION FOR THE GENERAL DATA PROTECTION REGULATION (GDPR)

Privacy legislation and regulatory compliance are always serious business, but the European Union's General Data Protection Regulation (GDPR) places formidable pressures on organizations, even those already following existing privacy rules.

Becoming GDPR compliant is not a task you should undertake alone. It involves people, process and technology working together to meet broad and rigorous requirements, and unprecedented scope. Unlike most legislation, its protection is based on citizenship, not geography.

Although it has been in effect since May 2018, it is never too late to tap the expertise you need to ensure compliance using a framework that reflects the realities of GDPR.

CONTENTS

GDPR is a Different Legislative Beast

GDPR was established by the European Parliament, the Council of the European Union (EU) and the European Commission to bolster and unify data protection for all individuals in the EU. It also deals with the export of personal data outside of the Union, so it encompasses the storage, processing and transmission of that information no matter where it resides.

GDPR's goal is to return control of personal data back to citizens and residents and simplify the regulatory environment for international business by unifying the regulations within the EU. Its creation was driven by several factors. There was already a great deal of data privacy regulation in place in developed countries, but it was not taken as seriously as it should have been. Enforcement mechanisms were not clearly defined and individual countries were challenged to enforce compliance on their own. The belief is that a single piece of legislation is more likely to be enforced as it is backed by 27 countries.

The long-term view inspiring GDPR was a perceived need for a global agreement on data privacy legislation, as organizations do not sufficiently respect the privacy of individuals. This is different from legislation conceived on a country-by-country basis, which has focused on what information can be transferred from one jurisdiction to another and where data is stored. Conversely, GDPR focuses on making sure the individual has some semblance of privacy in a hyper-connected world regardless of where their data resides.

The good news for organizations dealing with GDPR is that there are similarities between it and other privacy legislation – the Decision on Strengthening Network Information Protection in China, the Civil Internet Bill in Brazil, and Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, for example. This means previous compliance work can be repurposed to meet additional regulations.

It's the differences that are significant and understanding them is critical for compliance and necessary if the organization is to effectively operationalize within the parameters of GDPR.

The first is financial. GDPR imposes massive penalties of up to €20 million, or four percent of an organization's global earnings,

in case of a personal data breach. The second is the legislation's massive scope, applying to any organization that is conducting a transaction with any European citizen, rather than relying on where the organization is operating. GDPR essentially applies to every organization globally.

If you're running a hot dog stand in Chicago, GDPR says you are in scope because you may interact with a vacationing citizen from France who pays you with a credit card. Realistically, little can be done to enforce a fine on that hot dog stand should it not comply with GDPR, but the implications are massive. At the opposite end of the spectrum, a global online retailer such as Amazon is by definition in scope because it is undoubtedly selling to EU citizens. Compliance is necessary as GDPR greatly impacts your organization.

Despite GDPR's clarity on scope and penalties, unanswered questions remain. Its stated aim is to simplify the regulatory environment for international business, but it is unclear how it will change existing laws in EU countries. Do affected countries layer their own rules and penalties on top of the new legislation? Or does GDPR supersede an individual country's legislation? And while the penalties for non-compliance are clear in their severity, how the legislation will be enforced remains murky.

Broader Scope Means Bigger Ramifications

GDPR's radically different scope, based on citizenship rather than geography, is why its impact cannot be understated. It protects the privacy of EU citizens regardless of where they are, which means in reality most organizations are doing business in Europe even if they do not realize it.

Under country-specific privacy legislation, an organization can decide whether to continue operations in that jurisdiction based on a cost/benefit analysis because those laws are based on geography. Such an analysis makes little sense under GDPR because as the hot dog vendor scenario illustrates, any one of your customers could be an EU citizen.

The penalties for non-compliance also have more clout, and not just in terms of the fees imposed for non-compliance. What is often overlooked is that GDPR anoints data protection authorities with the duty and power to disclose any breach of personal information within 72 hours, whether it is one record or one million records. The inevitable bad press means an organization will be seen as derelict in its duty to protect the personal privacy of the individual.

The ensuing financial fallout due to the lost revenue that comes with a damaged reputation and fleeing customers overshadows GDPR's hefty fines, as well as the costs that arise from litigation. For example, retail chain Target reported more than US$191 million in overall expenses related to the data breach it suffered in 2013[1]. Meanwhile, Home Depot is only nearing the end of the litigation stemming from its 2014 data breach with a settlement submitted to court in March 2017[2].

The 2018 Cost of Data Breach Study: United States[3] found the average total cost of a data breach is $3.86 million. It also reports that the cost incurred for each lost or stolen record containing sensitive and confidential information is $148 per record.

If you do not have this data, then it cannot cost you money, and GDPR does provide guidance around retention. It stipulates that data subjects have a right to withdraw permission for use of their personal information. This is also commonly known as the right to be forgotten. Individuals can withdraw consent at any time, and the organization that originally collected the information must remove all information related to the data subject. A typical scenario is a retailer loyalty program. The retailer would need consent from the consumer to gather specific information, and further consent if the use of that information was to change. And if the consumer decides to no longer participate in that program, any data related to that person, including all copies, must be completely removed from all systems in such a way it cannot be recovered.

The right to be forgotten highlights the transformation required to operationalize the organization under GDPR. You must truly understand the lifecycle of every piece of information across systems, including the cloud, and how it is used and changed throughout its lifecycle. GDPR requires you to have a program that maps the movement of all customer data.

GDPR also puts pressure on organizations with new data processing requirements and touches on a few key areas:

- It requires that all data collected about an individual must be done in a transparent way.
- The scope of the data collected must be limited to specific and explicit data necessary for the task at hand, rather than collecting as much information as possible so it can be used for other activities.
- It mandates that organizations collecting data ensure it is accurate, raising questions about the degree to which organizations should be reasonably expected to ensure accuracy, given that a person could intentionally provide false information.
- Finally, GDPR mandates that data should not be stored any longer than it is needed. This recognizes that over-retention is a risk to consumer data, but how long data is "needed" is open to interpretation, raising the question of whether GDPR supersedes data retention requirements of other regulations.
- GDPR's requirement that you completely understand the entire lifecycle of your customer's data, combined with its broad scope and penalties for non-compliance, are all compelling reasons why you should prepare for it with the help of both internal and external expertise.

Put the Essential Pieces in Place: People, Processes and Technology

GDPR is in full swing. The breadth and scope of GDPR means your response is more than just another technology purchase. Processes and people play an equally important role if you are to effectively operationalize your organization under GDPR.

You should be looking at how compliance activities from existing legislation can support GDPR. From a people perspective, GDPR requires specific expertise in the short term to bring the organization to a state of compliance, and in the long term to maintain compliance. It is also a risk management issue that impacts an organization board of directors, executives, IT staff and every employee by requiring a culture that weaves security and privacy into daily operations. But more notably, the legislation stipulates the creation of a new role: the Data Protection Officer.

Organizations that practice large-scale data processing within special categories such as race, religion, biometrics and gender are required to appoint one or more Data Protection Officers. However, no concrete definition of "large-scale processing," is provided in GDPR, so this provision is open for interpretation.

The minimum duties of the Data Protection Officer are outlined:

- Act as the main point of contact for Data Protection Authorities
- Inform data controller or processor of what obligations they are required to adhere to
- Monitor compliance with GDPR
- Provide assistance where required for any Privacy Impact Analysis that must be conducted
- Cooperate with supervisory authorities and serve as a liaison between the organization and the authorities

The importance of getting the right people, including a Data Protection Officer, should not be discounted. It is a critical part of operationalizing the organization under GDPR. An accomplished Data Protection Officer, combined with a team of skilled employees and external resources, will save you money in the long run. They smooth the transition to compliance without disruption to your daily operations as you make the necessary adjustments to your business processes.

The expertise you assemble plays a key role in conducting the GDPR-mandated Privacy Impact Assessments necessary for evaluating new technologies or processes that impact personal data. As defined, a Privacy Impact Assessment must include the following elements:

- A description of the data processing operations and the purpose of the processing
- An assessment of the necessity of the data processing operations guided by why the data collection was authorized
- An assessment of the risks to the rights and freedoms of the data subjects
- The measures intended to address risks, safeguards, security measures, and mechanisms in place to ensure the protection of personal data and demonstration of compliance with GDPR regulations

The good news is many organizations already conduct similar risk analyses as part of their due diligence when acquiring a new technology. The Privacy Impact Assessment simply provides a guideline and establishes a minimum standard for such an assessment. It may be advisable to outsource this process to a third party.

This assessment will inform the user agreements that will have to be drafted so customers can provide consent around the use of the collected information, including a mechanism that allows them to withdraw that consent. The agreements can be similar to those that users face when installing software.

GDPR also presents itself as a legal issue, so your in-house counsel also plays a role. You should also tap the experience of external legal counsel that have practices devoted to privacy legislation. Their interpretation can help preparations and development of a framework to assist your organization in pulling together the essential components needed for compliance.

Create a Framework to Operationalize Under GDPR

Getting legal counsel involved is a good starting point for GDPR compliance, but your final framework should be an analysis of your organization conducted by a third party. Your primary goal is to operationalize GDPR.

A framework describes the information flows throughout your organization, identifies any risks to your data, and identifies and evaluates the risk mitigation. It provides the basis for all tasks that must be accomplished, whether or not they are explicitly defined by GDPR. The partner's analysis will provide the foundation for a framework that reflects the unique requirements of your organization, not just your industry, including the identification of your critical information assets and the true value they represent to your organization.

A knowledgeable, external resource is essential given the egularion scope, not just because of expertise, but because there is a great deal of work that must be accomplished to implement a successful program. Look for a partner that has the characteristics of a business consultancy combined with a strong understanding of technology, which is an enabler, not a silver bullet for compliance.

GDPR presents opportunities to consolidate systems. The framework not only guides decisions on new technology investments, but what you already have can be expanded in its use. For example, meeting the right to be forgotten requirement is a monumental task on its own, but can be aided by existing data loss prevention (DLP) technology. Your e-discovery tools can support the Privacy Impact Assessment.

CREATING A GENERAL DATA PROTECTION REGULATION FRAMEWORK

Creating a framework for GDPR compliance starts with a clear understanding of an organization's data, how it flows and how it is transformed.

A Critical Asset Protection Program (CAPP) provides the foundation for a GDPR framework. It enables identification of all data, including personally identifiable information (PII), as well as any other critical business data that may be in scope. It includes four key elements:

• Data Silo Controls: Information assets are cross referenced and mapped against security mechanisms, bearing in mind internal access and that the traditional concept of security perimeters no longer exists. GDPR compliance threats must be monitored between silos and users re-educated if necessary.

• Privacy Impact Assessments: This considers privacy by design and the right to be forgotten in any new systems, and the creation of plans so legacy systems include controls.

• Subject Access Requests: These should be established and not changed unless found to be excessive or unnecessary.

• Full Data Mapping: Conduct scheduled surveys and discovery scans regularly to identify data flows. This creates a live data asset map of PII attributes.

The four elements contribute to a program framework that supports compliance with GDPR, and is complemented by supporting technology. Ultimately, compliance is a continuum, so reviews should be conducted bi-annually to identify any lapses as they occur over time.

Not only can a partner help you make better use of technology, their understanding of GDPR's commonalties with previous legislation can help you with those requirements that are similar across jurisdictions. This will enable you to realize efficiencies while improving your overall compliance posture. With a framework in place, you will ultimately be well positioned to meet the specific demands created by GDPR.

GDPR Compliance is a Continuum

GDPR should not be taken lightly, and it could potentially become the global standard for data privacy protection legislation. Given its complexity and scope, you should have your technologies and data protection ramped up. Even those organizations who began preparations early should consider an outside partner to ensure a smooth transition to the new realities of doing business under GDPR.

Securing critical assets and protecting customer data is not a one-time project; it is a continuum of activities that reflects the realities of doing business in a digital, networked, global economy. Having a framework in place and a partner who understands both the legislation and the technology will enable you to operationalize your GDPR compliance. The transformation will make you nimble and well prepared to deal with any changes to GDPR, as well as any future regulatory changes and legislation you must adhere to.

---

1. McGinty, Kevin M. United States.
Privacy and Security Matters.
Target Data Breach Price Tag: $252 Million and Counting.
February 26, 2015
https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting/

2. CUNA News Now. United States.
CU Insight.
Home Depot settlement site available, claims due by Sept. 14
May 7, 2017
https://www.cuinsight.com/home-depot-settlement-site-available-claims-due-sept-14.html

3. Ponemon Institute LLC. United States.
2018 Cost of Data Breach Study: Global Overview
July 2018
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&