1105 MEDIA

FIRESIDE CHAT PAPER

Redmond
MAGAZINE

FIVE STEPS TO GDPR SUCCESS

By Jennifer Zaino

Is your business prepared to meet the May 25, 2018 deadline for compliance with the EU's General Data Protection Regulation (GDPR)? Most organizations aren't: 60 percent of businesses are at risk of not meeting the deadline, according to a recent report by Crowd Research Partners. While the majority of survey respondents considered it a top priority to become compliant with the rules that give EU citizens greater control over and protection of their personal data, their efforts are being held up by a lack of staff expertise and budget, as well as a limited understanding of the regulation.

Even at this late date, though, it is possible for organizations to take steps to better position themselves to support GDPR requirements.

GDPR: CHANGE BREEDS CONFUSION

While the regulation has its roots in the EU's Data Protection Directive of 1995 that addressed governing the privacy of individuals' personal data, the world has changed dramatically in the last quarter century. More personal data is being tracked and collected today than ever before. The Internet and smart phones have become mainstream, and so has everything from web site cookies that gather information about users' buying habits to mobile apps that acquire their location data. The Internet of Things (IoT) is well on its way to becoming a part of everyday life, too, with smart home devices and digital assistants able to accumulate customer data.

Individuals often benefit from companies having access to more of their personal information, of course. Products and services may be improved as a result of business' analysis of such data, for example. But GDPR changes the status quo that organizations have become accustomed to—that is, collecting and processing personal data to support business objectives.

Instead, as part of catching up past regulations to present conditions,

GDPR CHANGES THE STATUS QUO THAT ORGANIZATIONS HAVE BECOME ACCUSTOMED TO—THAT IS, COLLECTING AND PROCESSING PERSONAL DATA TO SUPPORT BUSINESS OBJECTIVES.

Cover: Maksim Kabakou / Shutterstock.com

GDPR mandates that EU citizens become the owners of their own data and in charge of what happens to it. Any organization that commands the collection of personal data from them—whether or not the operation is based in the EU—must respect principles including transparency, data minimization, storage limitations, and confidentiality, and can only do business with data processors who also implement controls for compliance with GDPR.

Key components of compliance requirements are that organizations deliver what GDPR terms “privacy by design,” creating processes with user data protection at their foundation, and that they ensure consumers’ rights to be informed about the collection and use of their personal data. Also on tap is giving individuals the ability to access and to rectify, erase, port or restrict the processing of their personal data. Companies also have to notify the proper authorities about personal data breaches within 72 hours of their occurrence.

Comprehending the differences between the GDPR’s definition of personal and sensitive personal data, and acting accordingly, adds further pressures. Personal data contains information to directly identify the subject, such as name and phone number, as well as pseudonymous data that doesn’t directly identify users but can identify individual behaviors. The latter is encouraged as a privacy-by-design method to support data-protection obligations. Sensitive data goes further, as it relates to race, health, political opinion, genetic and biometric data, among other things, and processing it is prohibited except under certain conditions.

GIVEN THE MANY DEMANDS OF GDPR, IT’S NOT SURPRISING THAT BUSINESSES ARE STILL STRUGGLING TO COMPREHEND ALL ITS FACETS AND HOW TO OPERATE UNDER THESE CONDITIONS.

Given the many demands of GDPR, it’s not surprising that businesses are still struggling to comprehend all its facets and how to operate under these conditions. They’re facing the challenges of incorporating new types of data, such as online identification markers, into privacy processes; classifying the user data they collect and process as personal or sensitive personal information across all departments; determining whether they have appropriate consent mechanisms in place to meet GDPR requirements for both classes of data; and developing methods to prove compliance with the regulation to auditors. Penalties are strict for non-compliance. For more details see https://www.gdpreu.org/compliance/fines-and-penalties/.

GETTING A GRIP ON GDPR

There's increased awareness that the clock is ticking for businesses in every industry and around the world to achieve GDPR compliance. But perhaps less considered is that it will keep ticking for organizations beyond the May deadline, as they must continually look to improve their implementation of GDPR policies, processes and practices as part of what really is an ongoing compliance journey.

THERE'S INCREASED AWARENESS THAT THE CLOCK IS TICKING FOR BUSINESSES IN EVERY INDUSTRY AND AROUND THE WORLD TO ACHIEVE GDPR COMPLIANCE.

How to successfully travel down this road? There are five key steps to follow, as outlined by data protection vendor Veeam Software, a global company that itself had to build a strategy and implement policies and practices for GDPR compliance.

The first two steps are critical, as they will make possible the protection of the personal and sensitive data a company controls and processes, as well as support the ability to document and continually enhance them.

Step 1: Everything starts with knowing your data. As much data as organizations collect, they're still a little sketchy when it comes to understanding the details—location, attributes and more. As businesses increasingly become data-driven, one might imagine that such particulars would be readily available. But the reality is that in today's world data may reside in multiple environments—the internal data centers of data controllers (the parties that determine the purposes and means of the processing of personal data), the private and public clouds they use, the SaaS services they subscribe to and even partner organizations that may aggregate or process personal data on their behalf. So, it shouldn't come as a complete surprise that an integrated, holistic process to account for all personal data doesn't always exist.

To that point, the biggest challenge and perhaps most substantial imperative is to understand the breadth and scope of all that data. Some of the information accumulated in diverse systems may give IT and data officers some new perspectives about getting in closer touch with their data.

Say, for instance, that the personal information of a German citizen who registered for a webinar hosted by a company's American marketing arm winds up in a SaaS solution licensed by that unit's line-of-business head—who neglected to inform IT about signing up for the service. The unexpected discovery that some of that citizen's personal data has been captured and processed can come as a jolt—not only because it was collected without IT's knowledge but also because no one previously had considered that a regional event aimed at U.S. users would attract the attention of an EU citizen. Knowing that rabbit holes like this exist in one department could spur deeper investigations into other business units outside of the EU that previously might not have been thought candidates for collecting GDPR-regulated data.

Bottom line: Don't make assumptions that EU citizen data will be where you expect it to be. Not all customer data will necessarily be in a central CRM system, for example, and some employee data might reside outside of an HR system. It's necessary to discover all the places that this data might be. So, conduct consistent surveys across all groups in the organization, including non-EU business units, to improve knowledge about whether they may be hosting GDPR-subject data. Create flow charts outlining the path of data across business processes—including its way in from third party partners or out to them—to help in understanding potentially non-obvious locations of EU citizen data, as well as for understanding your own businesses' and your partners' data boundaries. Make sure that all systems, even if not EU-centric, adhere to the same policies when it comes to classifying personal and sensitive personal data.

Step 2: Manage the data. With identification of what EU-subject data a business has and where, it's time to explore access control as the main component of data management. Compliance with GDPR demands knowing who in an organization uses EU citizens' personal and sensitive data and why, and whether their use conforms to permissions related to the application of that data.

AS A DATA MANAGEMENT PRIORITY, ACCESS CONTROL REQUIRES BUSINESSES TO KNOW WHO HAS ACCESS TO EU-CITIZEN DATA, WHY THEY NEED ACCESS TO THAT INFORMATION AND FOR HOW LONG, AND WHEN IT IS APPROPRIATE TO RESTRICT ACCESS.

As a data management priority, access control requires businesses to know who has access to EU-citizen data, why they need access to that information and for how long, and when it is appropriate to restrict access. For example, there shouldn't be an assumption that personal data collected by a hotel to reserve a room for a French national traveling to New York can be used by the company's marketing department to send her materials about the organization's worldwide locations that can service all her traveling needs. Once the legitimate business need for that data no longer exists, allowing access to it for other purposes could put a company in jeopardy of violating GDPR requirements.

To avoid issues, it's important to document the purposes for which the data was collected and restrict access to it only to the parties involved in fulfilling that objective during a specified timeframe. That holds true whether that data is processed and stored by the organization itself or by a third party who handles that function for them.

PROTECTING INDIVIDUALS' PRIVACY MEANS BUILDING PRIVACY-BY-DESIGN WORKFLOWS INTO SYSTEMS FROM THE START.

Building Off These Initial Steps

With these steps in place to set up an organization for meeting all aspects of GDPR compliance, businesses can take simultaneous actions to support other needs.

Step 3: Protect the data. There's no doubt that it's hard work to try and be consistent in data security efforts, such as vulnerability assessments and access restrictions, when data sprawls across internal systems and crosses over to external environments—those where the business may maintain control over it (public cloud) and those where it is less positioned to do so (SaaS).

Focusing on smart and consistent security policies rather than on physical security implementations can be an asset in promoting proactive security measures, even under these conditions. Doing so means the organization doesn't have to get too granular when it comes to the variables of security deployments across different environments and on different types of storage that host different types of data.

There's also the opportunity to draw closer ties between data protection and data management. For instance, companies can implement a "two-person" rule so that access to personal and confidential data requires that multiple individuals be involved in the access procedure for protection as well as auditing purposes.

Step 4: Document and comply. Protecting data also extends to proactively building in processes and leveraging technology to support backup and recovery as part of simple security workflows. It's critical to document these workflows so that the organization understands which managed or public cloud an EU citizen's personal data may have gone to in case of a disaster that required moving all data off-premise.

Protecting individuals' privacy means building privacy-by-design workflows into systems from the start and documenting them, as well, to fulfill EU citizens' requests to exercise GDPR-stated rights over their own data. That's a key part of removing complexity while enabling compliance. Its foundation lies in knowing where the data for an individual resides and centralizing that knowledge so that when an EU subject wants to be forgotten, for example, it will be simple to erase that data from all the systems that touched it. Simplified documentations and workflows also are crucial in making compliance stick in other scenarios—for instance, a database administrator may need to restore a database a week after an EU citizen's data was removed from it, and it must be assured that that data does not make its way back into the system.

Step 5: Review and improve. Given the fact that the GDPR compliance date is not the GDPR finish line, it's critical for organizations to continue to revisit their GDPR policies and processes, and how they accomplish them, to get the best results. Iteration and incrementation on GDPR implementations are the bywords here.

As an example, it's only through a follow-up review that a global organization may find that the surveys it initially conducted among business units to find out more about the data they held asked more probing questions for its EU divisions than it did for its other groups around the world. That can help it come to the realization that that model's lack of consistency has faults, because it won't uncover issues that may hamper GDPR compliance in these other locations. (Remember that example of the German citizen whose personal data wound up in a U.S. marketing organization's SaaS service!)

Striving for global consistency—in surveys and workflows—as part of GDPR iterations makes an organization better able to respond to changes in GDPR regulations as well as to the business' own evolution. An enterprise that acquires another company needs to make sure that the acquired company quickly becomes inclusive of its own GDPR policies and processes, for instance.

The good news is that regulations like GDPR don't have to inhibit a business' goals but can indeed complement them. Supporting these security and privacy regulations—and perhaps even extending them to all individuals and not just EU citizens—can help an organization build more trust with its user base. In today's environment, where individuals everywhere have increased concern about what's happening with their data, it's a plus for any company to show that it's working hard to keep faith with its customers.

Find out more
http://veeam.com/wp-gdpr-compliance-experience.html

Veeam