Bloomberg Law

Privacy and Security Law Report®

GDPR Compliance

The European Union General Data Protection Regulation is an opportunity to retool information technology in essential ways, and it's an opportunity to reap the significant benefits of that retooling—including reduced risk, reduced costs and better business performance, the author writes.

GDPR: IT's High-ROI Security Opportunity?

BY AL MONSERRAT

There are several ways to view the European Union's General Data Protection Regulation (GDPR). Most organizations' response ranges from anxiety to indifference. Some information technology leaders, however, have taken a unique approach and view it as an opportunity to increase their risk on investment (ROI) on technology investments.

Most European business leaders view GDPR with anxiety and resignation. The anxiety is because GDPR sets forth some fairly rigorous mandates for safeguarding the security of EU customer and employee data and giving these individuals control over that data—while also threatening financial penalties of up to 4 percent of a company's annual worldwide turnover for compliance failures.

The resignation is because business leaders know there's no fighting GDPR. By May 25, 2018, their organizations must be GDPR-compliant. So, they have to spend whatever it takes to fulfill the operational requirements of GDPR and ensure their ability to survive a GDPR audit.

In the U.S., many organizations still view this as a low priority in their 2017-2018 strategies and have yet to begin planning—but time is running out. They must realize that any global organization—even if they are headquartered in the U.S.—must comply if they have customers in an EU country or employing EU citizens. There's also a good chance that GDPR-like mandates will emerge in the U.S. either as new legislation or as extensions of existing regulations such as PCI data security standards and the Sarbanes-Oxley Act.

There is, however, another way to view GDPR—is also an opportunity. It's an opportunity to retool IT in essential ways. And it's an opportunity to reap the significant benefits of that retooling—including reduced risk, reduced costs and better business performance.

Al Monserrat is chief executive officer at RES, a digital workspace technology company.

Global Data Stewardship for a Global Digital Citizenry

To understand GDPR as an opportunity, it is first necessary to recognize the epochal shift occurring in the nature of data itself. Data is no longer just something that companies use for their own internal purposes. It has become a universal medium of value exchange.

Companies sell data and buy data. Stolen personal data is sold in open markets with money-back guarantees. And, increasingly, customers see data about themselves as a personal possession of value—over which they have a right to exercise sovereignty similar to that which they exercise over their finances, their possessions and even their persons.

To view the GDPR as just a burdensome regulation by an out-of-control bureaucracy, is to miss out on a

transformational opportunity. It is a harbinger of social, cultural and economic change that requires business leaders to completely re-think their stewardship of data in the context of an empowered global digital citizenry. All businesses, in effect, are becoming like banks—except instead of being entrusted with customers' money, they're being entrusted with customers' data.

Anyone who doubts that the relationship between their business and their customer data is changing need only consider GDPR's specific provisions. Customers can now tell you what you can and can't do with their data. They can tell you to delete their personal data if they so choose. And if you fail to comply, the cost will be more than a disgruntled ex-customer. It will be millions of dollars.

Personal data sovereignty is coming to the U.S. too. It may not immediately come in the form of regulation precisely equivalent to the EU's GDPR. But it's inevitable. Identity theft protection services are evolving into identity sovereignty services. Companies explicitly inform their customers about not selling their data to third parties. And every new headline about a corporate data breach elevates the issue as a public policy concern.

The bottom line: your business performance will be directly affected by the effectiveness and efficiency with which you manage customer data. So the investments you make in GDPR compliance can have much broader upside payoffs—if they're the right ones.

Five Keys to GDPR ROI

Five areas of investment are especially important for ensuring effective, efficient compliance with GDPR mandates while gaining broader benefits for the business:

Key Investment #1: Good Data Governance

You can't effectively protect and manage your customers' personal data if you don't know exactly where it is.Therefore, diligent disciplined data governance is a must for any GDPR compliance effort. This will also ensure that you can make the most valuable connections between and across the data.

Unfortunately, most organizations have relatively weak data governance practices. Users can grab all kinds of data and put it into personal Excel spreadsheets that aren't tracked or well-secured. Application developers tap into databases to test their code—and then never bother to clean up those test instances behind themselves when they're done. Data also gets pulled into data warehouses, data lakes and other aggregations for analytic and business intelligence purposes. That data then gets replicated over and over, with each new instance being treated as if it were a primary source.

You can't effectively protect and manage your customers' personal data if you don't know exactly where it is.

None of this is good for GDPR compliance or for the digital enterprise in general. Every business needs to know where all of its data is, what all of its data is, and where that data originated. Businesses also need to define and enforce policies regarding how data is used, viewed, copied and accessed. Many businesses keep tighter control over their petty cash and their office supplies than they do over their data. That must change in response to both GDPR and the broader shift in the value of data.

Key Investment #2: Context-Based Mobile Workspace Controls

The ascendance of data is taking place at the same time as the ascendance of mobile. Employees take their digital identities with them wherever they go, and they expect to be able to get their digital work done regardless of their physical location or time of day. In fact, we demand that people work over the weekend or on the go from their smartphones, tablets, laptops and home desktops.

This is a problem for organizations that continue to depend on static, perimeter-based technologies to control access to sensitive data resources. Mobile data access management requires much more than that, including the ability to answer and appropriately respond to questions such as:

- Is the mobile user who they claim to be?
- Are they connecting with a known or unknown device?
- Are they connecting via a trusted or untrusted network?
- Are they using unrecognized or company-sanctioned USB drives or peripherals?
- Are they attempting access during business hours or at an unusual time of day?
- Are they attempting access from an unusual physical location?

The collective term for these questions is ''context.'' The only way to ensure that customer data doesn't travel anywhere it shouldn't travel—and that all use of customer data is legitimate and traceable—is to manage data access in context. Context and associated policies determine what is and isn't allowed. It also provides the usage data essential for GDPR audit reporting.

Key Investment #3: Streamline Privilege Administration With Automation and Delegation

Over time, people tend to wind up with much more access privileges than they need. This is the result of two forces intrinsic to almost every organization. The first force is the appetite people have for more privilege, rather than less. No one ever calls IT to say ''Can you please reduce my access?'' Instead, they always want more.

In some cases, privileges are justified. IT administrators, for example, often need privileged accounts to perform management tasks. line of business managers and project leads may also require privileged access to get the data they need, when they need it.

The second force is inertia. The granting and revocation of privileges is typically a manual process. So once someone is given an elevated privilege, they tend to keep it. IT staff also often give users a bit more privilege

  PVLR ISSN 1538-3423

than they need in order to avoid potentially bothersome additional subsequent requests.

The net result: lots of people have lots more privileges than they need. And that creates serious risk exposures when it comes to GDPR—as well as cybersecurity more broadly.

The solution to the problem of creeping privilege is to streamline administration of access rights. This streamlining can largely be accomplished through automation. The right kind of automation makes it much easier for IT administrators to quickly and easily give users precisely the rights they need at any given. Automation also enables IT to put a ''freshness date'' on privileges so they don't persist indefinitely.

Organizations can also fight privilege creep by using delegation tools that empower line-of-business managers, human resource administrators, and other non-IT stakeholders to perform access administrative as appropriate. For example, a regional vice president could give a data analyst helping with a new marketing project access to a customer database. That privilege could then automatically end after 60 days.

This adaptive, business-aligned approach to access control can significantly reduce total organizational privileging without impairing anyone's ability to be productive.

Key Investment #4: Anti-Ransomware Whitelisting

One of the biggest threats to high-value data is ransomware. Ransomware attacks impact about half of all companies, and they keep getting more sophisticated. These attacks often take the form of ''spearphishing'' and other social engineering techniques that circumvent cybersecurity perimeter defenses by tricking human users into clicking a malicious link or opening a malicious attachment.

Effective ransomware defense requires multiple counter-measures, including frequent data backups and aggressive user education. However, any organization seeking to fend off ransomware and similar cyberattacks must also implement some form of workspace whitelisting.

Whitelisting entails denying access to all non-approved resources by default. So instead of having to specifically identify malicious hosts with 100 percent accuracy, IT simply keeps malicious hosts off users' whitelist.

Companies that diligently prepare for General Data Protection Regulation compliance by making the investments above will reap significant financial returns.

For whitelisting to work in the real world, though, users' whitelists must reliably include all the resources they need to do their jobs. Otherwise, whitelisting erodes productivity at the same time as it strengthens security. Effective whitelisting is thus closely related to automated privilege administration (key investment #3)—with the added dimension of disallowing access to non-whitelisted resources.

Key Investment #5: Push-Button Offboarding

Another related and essential capability for GDPR compliance is push-button offboarding. As noted above, users can accumulate lots of access privileges over time. So when they quit, get fired, fall ill or leave their position for any other reason, those privileges must all be revoked.

Unfortunately, as with other aspects of user administration, this revocation can be slow, manual, and unreliable. In fact, it's not unusual for some user privileges to remain in place for weeks or even months after they've been terminated.

This is a no-no for GDPR and for data security generally. Disgruntled employees can do a lot of digital damage if they still have the privileges they need to do so. And failure to revoke privileges can itself be considered a compliance violation, even if no one actually does anything inappropriate.

Every organization therefore needs an offboarding mechanism that triggers complete revocation of all privileges across all systems—on-premise and in the cloud—without exception immediately upon a termination or transfer event in the company's HR system.

The GDPR Prep Payoff

Companies that diligently prepare for GDPR compliance by making the investments above will reap significant financial returns. Those returns include:

- **Better data- and analytics-driven decision-making**—Data governance best practices don't just support regulatory compliance. Those practices also help ''democratize'' data by making it easier for IT and non-IT stakeholders across the enterprise to pinpoint the data they need and place an appropriate level of confidence in its accuracy. The result is better, broader use of analytics across the business.

- **Long-term customer/brand loyalty**—Customers are getting smarter and more concerned about how companies treat their personal information. Businesses that don't take their responsibility for protecting PII seriously will quickly and permanently alienate these customers—GDPR or no GDPR. Diligent data stewardship, on the other hand, will help businesses build a differentiated digital brand.

- **Greater organizational agility**—Policy-based automation of user access to digital resources enables IT to respond much more quickly and easily to all kinds of change—including acquisitions, mergers, and reorgs. So GDPR investments payoff can repeatedly payoff in both hard operational savings and faster M&A time-to-benefit.

- **Reduced cybersecurity risk**—Given the relentlessly increasing intensity of cyberattacks, the value of improved security should not be taken lightly. Measures taken to fulfill GDPR mandates pay off handsomely as added layers of security—especially when it comes to threats such as ransomware and inside jobs.

- **Higher-value allocation of IT staff**—The same automation that brings policy-based control to users' desktop and mobile workspaces also frees IT staff from low-value manual tasks. Given how difficult it is to recruit and retain highly skilled, highly motivated technical talent, this improved allocation of human resources

can save money and empower organizations to better leverage technology—rather than constantly being bogged down in IT ''housekeeping.''

■ **Reduced overall compliance and audit costs**—GDPR is not the only regulation to require auditable controls of user access. In fact, future regulatory audit requirements for user access will almost certainly escalate regardless of how the political landscape may change. Well-governed data and policy-based workspace controls make that kind of audit reporting vastly easier, cheaper, and more credible.

■ **Avoidance of GDPR-related fines**—This is an obvious primary benefit, but it shouldn't be minimized. If you have customer in Europe, GDPR applies to you. So do the substantial potential penalties for non-compliance.

Not every GDPR initiative will reap these benefits. Companies that approach GDPR compliance as a siloed project that merely attempts to check off boxes on a checklist with as little cost and effort as possible may not achieve significant improvements in cybersecurity, operational efficiency, or brand value. They may even also fail to pass their GDPR audits.

But those that properly view GDPR as one small part of a broader effort to better govern data the digital enterprise—traversing compliance, security, and automation—will significantly out-perform their more complacent competitors. And that performance will definitely have a tangible, positive impact on the bottom line.

  PVLR ISSN 1538-3423