CDW PEOPLE WHO GET IT®

FINANCE AND GDPR: WHAT YOU NEED TO KNOW

Banks, credit unions, capital markets firms and others must understand the EU's new privacy regulation in order to comply with it.

EXECUTIVE SUMMARY

In May 2018, the European Union's long-awaited General Data Protection Regulation (GDPR) went into full effect, updating privacy regulations throughout the EU and creating ripple effects felt around the world. GDPR lays out the basic premise that individuals should have control over their own data and places new restrictions on financial institutions and other organizations seeking to store, process or transmit that data.

The implications for financial institutions are profound, requiring that firms understand how they interact with personal information and obtain consent from individuals before taking action with that data. The major shift is that data processors must now incorporate data protection "by design and by default," meaning that they must consider data protection when designing any business process, and all actions they take must have a default assumption of privacy.

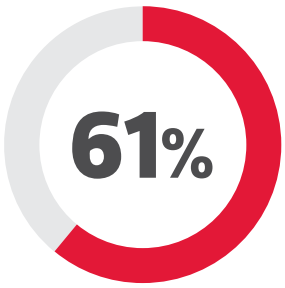
The financial industry is still coming to grips with the true implications of GDPR and is eagerly awaiting the case law that will inevitably clarify the standard. In the meantime, financial institutions seek to implement policies, strategies and technologies that will position them to comply with GDPR as well as an expected wave of other global regulations.

What Is GDPR, and How Does It Affect Financial Institutions?

The General Data Protection Regulation (GDPR) is a broad-based privacy regulation that is intended to create a consistent framework for handling personal information throughout the European Union and reaches across international borders to regulate usage of that information worldwide.

Each of the 28 EU member states has its own implementing legislation that applies the GDPR framework within its own legal system and creates any exceptions that might exist in each country. For example, the Data Protection Act implements GDPR in the United Kingdom, while the similarly named Data Protection Act 2018 implements it in Ireland. Latvia has the Personal Data Processing Law, while Austria implemented GDPR by amending its Data Protection Act 2000.

Financial institutions are no strangers to privacy regulations, operating in one of the most heavily regulated industries in the world. The most important implications of GDPR for institutions already steeped in privacy practices will be to ensure that their current operations comply with GDPR's provisions, to extend privacy practices to new categories of information, and to determine that they have appropriate controls in place to demonstrate compliance to regulators and auditors.



The percentage of companies that see benefits beyond compliance associated with GDPR remediation activities[1]

What Types of Personal Information Does GDPR Cover?

GDPR creates two categories of personal information that companies must protect. The first broad category is simply "personal data," which is defined in GDPR Article 4 as "any information relating to an identified or identifiable natural person." This includes virtually any data collected about a person that can be somehow linked back to that person, even if it doesn't have a clear identifier.

The second, and more restrictive, type of personal information consists of data elements that fit into the "special categories" of personal data defined in GDPR Article 9. These include information about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. This category also includes genetic and biometric data and information about a person's sexual activity or orientation. Organizations are prohibited from collecting or processing this type of information unless the use fits within one of 10 narrowly tailored exceptions.

It's very important to note that, while GDPR is a European law, it has reach far beyond the borders of the European Union. While it clearly applies to the data processing activities of companies based in the EU, GDPR's provisions also apply to any organizations that handle information covering EU residents. This includes financial institutions in the United States that have EU residents as customers.

Why Did the EU Impose This Regulation?

The European Union has long been a leader in creating data privacy legislation, and the influence of EU privacy law is felt globally. The origins of privacy regulation in the EU are found in a 1980 document authored by the Organization for Economic Cooperation and Development (OECD) covering the flow of personal information across borders. This document outlined seven key principles for handling personal information:

- **Notice:** Data subjects should be notified when their information is collected.
- **Purpose:** Data collected should be used only for the purpose agreed to by the subject.
- **Consent:** Data subjects should have the right to restrict the flow of their information.
- **Security:** Stored data must be protected against threats to its confidentiality and integrity.
- **Disclosure:** Data subjects should be informed of any changes to the processing of their data.
- **Access:** Data subjects should have the right to review information about them and correct any errors.
- **Accountability:** Data processors should be held accountable for compliance with these principles.

OECD is a nongovernmental organization and does not have the ability to make law, but the principles it outlined were embraced by the EU in 1995 when it adopted the European Union Data Protection Directive (DPD) as EU Directive 95/46/EC. The DPD served as the first international legal framework for protecting personal information and served as the impetus for organizations around the world to adopt privacy protection standards, many for the first time.

After two decades under the DPD, the European Union sought to enhance protections around personal information and adopted the GDPR as its new privacy framework. The organization's intent was to harmonize existing data privacy rules across the European Union while making it easier for EU residents to understand how their data is being used. GDPR also provides a consistent mechanism for reporting and investigating potential violations. At a high level, GDPR is intended to ensure that consumers retain power over the collection and use of their personal information.

The European Council adopted the GDPR as law on April 14, 2016, and set a timeline for implementation that allowed member states two years to adopt implementing legislation. The final GDPR compliance deadline passed on May 25, 2018.

What Effect Will It Have on Financial Organizations?

Financial institutions must comply with GDPR, as must any organization doing business in the European Union or with EU residents. However, financial institutions are uniquely positioned to comply with GDPR because they've already been subject

Source: "The Time is Now: The Deloitte General Data Protection Regulation Benchmarking Survey," 2017

to a wide variety of global privacy regulations. Many of the data governance practices already put in place by the financial industry serve as the basis for GDPR compliance programs.

The most significant effects of GDPR relate to the technical controls used to protect client information. At a high level, financial organizations will need to:

- Build an inventory of personal information held by the organization, including the nature of the information, the locations where it is stored and the purpose of the collection.
- Obtain clear consent prior to collecting and processing personal information.
- Establish processes to enforce an individual's right to data erasure and right to be forgotten.
- Implement pseudonymization controls to remove a subject's identify from personal information prior to sharing, whenever possible.
- Manage the flow of information to vendors and through third-party information systems.
- Develop breach notification processes.

These controls serve as the basis of a GDPR compliance program and also provide a solid foundation for protecting the privacy of personal information.

How Is the Regulation Being Enforced, and What Are the Penalties for Noncompliance?

Every EU member state designates a supervisory authority responsible for enforcing data privacy rules and investigating cases where organizations are not compliant with GDPR. The reason GDPR has attracted so much attention is that these supervisory authorities have the power to levy substantial fines. When assessing a fine, GDPR requires that the supervisory authority consider a number of factors, including:

- The nature, severity and duration of the infringement.
- The intentional or negligent character of the infringement.
- Any action taken by the infringing organization to mitigate the damage.
- The nature of the technical and business process controls put in place by the infringing organization.
- The past record of violation by the infringing organization and its degree of cooperation with the investigation.

The penalties assessed by GDPR are progressive. Larger organizations will face larger maximum fines, ensuring that the impact of a GDPR violation will be significant even for enormous multinational corporations. In the case of the most severe breaches, supervisory authorities may assess a fine of up to 20 million euros or 4 percent of the organization's worldwide revenue, whichever is higher. For example, a multinational corporation with 100 billion euros of worldwide revenue would face a maximum fine of 4 billion euros.

The Impact of GDPR

Financial institutions across the United States are beginning to feel the effect of GDPR on their routine operations. While most financial organizations already have robust privacy practices due to existing U.S. laws and regulations, GDPR compliance still requires the attention of security and privacy professionals to ensure that their firms remain on the right side of the law. Many industry observers feel that the supervisory authorities in EU member states will begin handing down some significant fines over the next year in order to demonstrate that they are serious about enforcing GDPR. Financial institutions are prime targets for these fines, given their high-profile operations and deep financial reserves.

How Does GDPR Affect Other Regulations of U.S. Financial Organizations?

Financial organizations already operate in a heavily regulated environment in the United States, and those regulations often directly touch on the same issues covered by GDPR. It is crucial that each firm consult legal counsel to determine how GDPR compliance intersects with their existing compliance obligations, based on the specific operating circumstances of the firm. No one-size-fits-all solution to GDPR compliance exists.

In most cases, U.S.-based firms should take the position that local laws will have precedence over GDPR in most cases. The provisions of GDPR will only become relevant when the operations of those firms touch the data of EU residents. The European Commission is not attempting to gain jurisdiction over data belonging to the residents of the United States or other non-EU states. That said, the simplest path to GDPR compliance for some may be to adopt GDPR-compliant policies worldwide.

Fortunately, most financial institutions already have a head start on their compliance efforts because of their existing practices under the Sarbanes-Oxley Act (SOX) and the Payment Card Industry Data Security Standard (PCI DSS). These long-standing regulations include provisions that directly complement the provisions of GDPR.

SOX became law in 2002 to increase the transparency of data regarding publicly traded companies, including many financial organizations. Like GDPR, the reach of SOX is felt outside its natural jurisdiction, as companies around the world have adopted

How Are U.S. Organizations Complying with GDPR?

Organizations had two years to prepare for GDPR, but the provisions of the regulation often required significant changes to business processes and information systems. This was especially true for organizations outside the European Union that found themselves wrapped into the provisions of the EU privacy regime for the first time. As the May 2018 deadline approached, some organizations struggled to comply with the regulation.

The business analytics firm SAS conducted a survey of organizations as the deadline approached in April and found that only 7 percent were already compliant with GDPR with only a few weeks remaining before the deadline. Only 46 percent of overall organizations believed that they would be compliant by the deadline. There was also a striking geographic disparity in those numbers: While 53 percent of EU-based organizations believed they would be ready for the deadline, only 30 percent of U.S.-based organizations felt the same way.

SOX standards as their normal operating practices.

The PCI DSS is a private regulation among participants in the credit card processing system that went into effect in 2004. Like GDPR, PCI DSS aimed to enforce security requirements for sensitive information. PCI DSS focused specifically on payment card information, while GDPR has a much broader mandate to include all personal data. Organizations with experience handling PCI DSS issues will be relieved to learn that GDPR is far less prescriptive than PCI DSS. While GDPR provides guidance on the types of information that must be protected, it does not provide a detailed set of requirements. PCI DSS, on the other hand, has a very narrow scope but provides extremely detailed requirements on how organizations must protect payment card information.

Financial institutions that are already PCI DSS compliant may consider taking the practices they have implemented around payment card information and extending them to the rest of their business. These same controls and processes may serve as a head start in meeting the confidentiality and integrity provisions of GDPR. Some of the specific areas that financial institutions should address include:

- Discovery of personal information throughout the organization
- Implementation of secure data handling practices for personal information
- Tracking compliance with GDPR and other mandates
- Handling customer requests for information
- Responding to and reporting data breaches

The key to integrating GDPR into other compliance efforts is recognizing that the focus of GDPR rests in data transparency, portability and consent. Consumers must be granted control over their personal information.

What Is a DPO, and Why Should You Assign One?

GDPR requires that organizations fitting into several categories appoint a data protection officer (DPO). These categories include government agencies and organizations that process special types of personal information. Financial institutions normally won't fit into two of these groups, but they may fit into the third: organizations conducting core activities that "require regular and systematic monitoring of data subjects on a large scale." Financial organizations should consult with their attorneys to determine whether they require a DPO, although it is considered a best practice to appoint one.

The role of the DPO is set forth in GDPR Articles 37–39. Organizations appointing a DPO must select an expert in privacy regulation and provide him or her with the resources and leeway to carry out the data protection program. The DPO cannot be a perfunctory position buried within the organizational chart. GDPR requires that the DPO report directly to the most senior executive in the organization. It also prohibits the organization from interfering with the work of the DPO or punishing the DPO for carrying out the function properly.

What Effect Does GDPR Have on Legacy Systems?

Financial institutions often operate legacy systems that run on outdated technology while performing critical business functions, including the handling of personal information. Technology teams often make compromises around securing these systems in the interest of keeping critical operations moving along. However, GDPR does not draw any distinction between brand-new systems designed with privacy compliance in mind and legacy systems. Both must operate in a manner that is fully compliant with the law.

GDPR marks a turning point for many legacy deployments. Technologists and business leaders face the choice of either continuing to invest in prolonging the life of legacy systems or using GDPR as an impetus for change and launching new systems that incorporate privacy by design as a core principle. These systems must not only protect privacy, but also ensure the accuracy and portability of personal information and facilitate the processing of user requests to review information or be forgotten.

As with many technology dilemmas, the decision between these alternatives hinges on cost and resource availability. Financial organizations should conduct a cost-benefit analysis and decide whether the time has come to replace their legacy applications.

Dealing with GDPR

As financial institutions undertake their GDPR compliance efforts, they may take advantage of a wide range of technology controls, third-party services and policy revisions designed to help them achieve compliance. One primary consideration that firms must keep in mind is that GDPR is not primarily a technology issue. Rather, GDPR requires that organizations think carefully about the policies and business processes that surround the handling of personal information.

What Key Technologies Can Help Financial Organizations Handle the Requirements of GDPR?

While financial institutions should approach GDPR as a business problem, several technologies can play a crucial role in achieving and maintaining GDPR compliance. These tools automate the routine work of compliance and serve as tracking tools to help the firm monitor its ongoing compliance efforts.

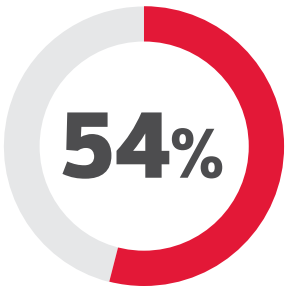
Electronic discovery tools have traditionally assisted organizations in identifying and preserving information that is subject to legal disclosure requirements. They comb through diverse information sources and perform keyword matches to discover hidden troves of information locked away on a desktop or server, in an email account or uploaded to a cloud service. These tools can also be used for GDPR tasks, helping an organization identify stores of personally identifiable information (PII) as it builds a data inventory. After locating information with a data discovery tool, business leaders may then map the flow of information throughout the organization and decide to either purge it or obtain appropriate consent. These tools may also play an important role in finding references to an individual who has requested access to information or is exercising his or her right to be forgotten under GDPR.

Advanced threat monitoring and protection tools also help to enhance an organization's security posture by building profiles of normal activity and then detecting deviations from those behaviors. The use of these tools boosts the level of insight into security activities and assists with the breach detection and response provisions of GDPR.

GDPR compliance frameworks are designed for the specific purpose of storing and tracking compliance-related information. They monitor the user consent process and track compliance activities throughout the customer lifecycle. Compliance frameworks replace the manual tracking that many organizations currently perform in spreadsheets with an auditable solution that provides external auditors with the confidence the organization is carefully managing GDPR compliance.

Subject access request portals also provide a boost to GDPR compliance efforts by offering a single interface to receive, track and respond to requests for information, as well as the exercise of a consumer's rights over personal information. These portals track the full lifecycle of consumer requests and assist the organization with responding within legally mandated time frames.

These are just a few of the technologies that can assist organizations in complying with GDPR. Organizations may also draw upon a wide range of existing tools to improve the security of their data processing environments. These include encryption for data at rest and in transit, as well as enhancing the security of workspaces, data centers and networks.



The percentage of companies that say the potential for large fines makes a difference in how they approach GDPR[1]

What Services Can Third Parties Offer to Help?

As financial institutions move to implement GDPR-compliant practices, providers have stepped up to offer services that assist with compliance efforts. In addition to compliance frameworks and subject access request portals, many firms offer GDPR compliance services to help organizations review their obligations and implement compliant business processes.

Law firms play a pivotal role in compliance efforts, helping financial institutions review their practices in the context of GDPR. Attorneys may also review compliance policies and ensure that an organization takes a standardized approach to compliance. They can also help sort out the precedence of overlapping privacy regulations from different jurisdictions.

In additional to turning to service providers for legal help, GDPR also permits organizations to hire a DPO on a contract basis. In cases where an organization fills the DPO role with a contractor, it must disclose the details of the arrangement to its supervisory authority.

In all cases, organizations must remember that they are themselves the data controllers and processors subject to GDPR. They may delegate the authority to act on their behalf in privacy matters, but they cannot delegate the accountability and responsibility for GDPR compliance. When firms engage third-party service providers, they remain liable for any failure to comply with the law's provisions.

What Policies Should Financial Organizations Consider Implementing or Changing?

As a regulation that focuses on business processes, GDPR often requires that organizations adjust their existing policies or adopt new policies related to personal privacy. These include provisions around the design and implementation of systems and processes as well as employee training and awareness efforts.

One of the guiding principles of GDPR is that data processors should adopt approaches that incorporate privacy practices "by design and default." Privacy by design simply means that privacy should be a foundation of any system or business process. Designers should use the technical and administrative controls at their disposal to build privacy requirements into their designs from an early stage. For example, designs should embrace the principle of minimization to reduce the amount of personal information collected and retained by an organization.

Privacy by default means that organizations should adopt practices that assume individuals will want to preserve the privacy of their information. This principle applies to the amount of information that a firm collects, the types of processing it performs, the length of time it retains data and the access it allows to personal information. Institutions must design systems that, by default, do not make private information accessible to the public without the subject's specific approval.

Website Privacy Practices

The most visible impact of GDPR comes in the privacy notices that appear on websites throughout the European Union. Anyone arriving in the EU will immediately notice when loading their browser that virtually every website they visit now bears a banner explaining the organization's privacy practices, particularly with respect to the use of tracking cookies.

Organizations that operate websites accessible in Europe should include a full disclosure of their privacy practices on the site and use these banners to inform users of their use of tracking cookies. It is acceptable to show these banners only to users subject to GDPR, but it is often simpler to adopt privacy practices on a sitewide basis.

In addition to disclosing the use of cookies and the collection of information, financial institutions should offer website visitors the ability to opt out of these practices on a full or partial basis.

Source: "The Time is Now: The Deloitte General Data Protection Regulation Benchmarking Survey," 2017

The requirements of GDPR have an impact on the daily routines of employees throughout an organization. Financial firms should adopt training and awareness policies requiring that anyone who comes in contact with PII receive recurring reminders of their responsibilities and the organization's privacy practices.

Before creating new privacy policies specifically for GDPR, financial institutions should examine the policies put in place for SOX and PCI DSS compliance. Those policies may already cover many of the organization's GDPR obligations, and it may be sufficient to tweak those policies to fill any remaining gaps.

CDW: A Finance Partner that Gets IT

CDW's solution providers serve as your organization's GDPR compliance partners. CDW's large and experienced finance practice includes experts on a wide variety of technology challenges facing financial organizations and is well-versed in GDPR compliance strategies.

CDW's GDPR services include three different offerings at basic, essential and premium service levels. The basic package is an awareness engagement that allows an organization to understand its risks and obligations under GDPR. It also includes an assessment of whether an organization's external websites are compliant with the regulation.

The essential package goes a step further and includes a series of workshops and data gathering exercises designed to assess GDPR compliance. It also includes a high-level technical strength engagement where CDW reviews the firm's existing security policies and technologies to produce a gap report for GDPR compliance.

Finally, the premium package includes all of the services in the basic and essential packages but then moves on to provide advanced compliance activities. These include data mapping activities, the design of data protection impact assessment templates and the creation of compliance tracking tools.

The CDW Approach

ASSESS

Evaluate business objectives, technology environments and processes; identify opportunities for performance improvements and cost savings.

DESIGN

Recommend relevant technologies and services, document technical architecture, deployment plans, "measures of success," budgets and timelines.

MANAGE

Proactively monitor systems to ensure technology is running as intended and provide support when and how it is needed.

DEPLOY

Assist with product fulfillment, configuration, broad-scale implementation, integration and training.

Explore Our Featured Partners:

aruba a Hewlett Packard Enterprise company

cisco Partner Gold Certified

FireEye

Symantec

To learn more about how CDW can help your financial institution deal with GDPR and other regulations, visit CDW.com/Finance or schedule a consultation with a CDW expert at 800.800.4239.

CDW PEOPLE WHO GET IT®