The MPI Group
People. Purpose. Profits.

The Finance Industry and the GDPR

New Standards, New Risks — and New Opportunities

Brought to you by Canon U.S.A., Inc.

Canon

www.cusa.canon.com

The U.S. finance industry faces immense challenges from the European Union's General Data Protection Regulation (GDPR). Financial services companies already account for a high percentage of institutional data breaches and cyber-crime costs, and the GDPR may further complicate the sector's compliance strategies for collection and handling of personal information. Yet amid general concern and uncertainty in the finance industry about GDPR compliance, some companies see opportunity.

Why?

Because leaders at these institutions understand that streamlined information workflows can not only help with security and GDPR compliance efforts, but also help them to serve their clients better and deliver a competitive edge. With new best practices and technology-enhanced information workflows, financial institutions can become more responsive, agile, and efficient — and create models for personal information management that can serve them for years to come.

New Standards and New Risks

U.S. financial institutions hold vast amounts of private information, much of which can be subject to the purview of the GDPR, such as:

- EU customer records
- EU account statements
- EU employee records
- Job applications from EU individuals
- Online banking/investment access information
- Research containing EU personal data
- Communications with — and marketing to — EU individuals (website, email, Facebook, etc.).

In response to individuals' demands for greater control over their information, including understanding who holds and uses it, other privacy regulations are also emerging around the globe, sometimes modeled on the GDPR. The array of penalties that governments can impose on financial institutions to protect personal information has increased as well in some jurisdictions.

After decades in the making and a two-year period for organizations to prepare, on May 25, 2018 the European Union began enforcement of the GDPR. Some consumers and privacy rights activists argue that laws such as GDPR are long overdue, with regulators lagging behind technological advances. This means that while GDPR compliance may seem daunting now, tomorrow it could likely be viewed as just another cost of doing business in the EU — or anywhere.

GDPR covers the "protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of such data,"[1] and can dramatically increases personal-data security responsibilities and risks for businesses of all types (*see GDPR Basics).* Even more significant is GDPR's establishment of new standards for data privacy rights that other lawmakers may try to replicate. For example, in June 2018, California passed a digital privacy law, effective January 2020, that gives consumers more control over their personal infor-

[1] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

[2] California Consumer Privacy Act, caprivacy.org.

mation that covered businesses collect from them online.[2] And as inappropriate uses of personal data by holders and hackers continue to make news, increasingly stringent regulations may arise.

The California Consumer Privacy Act reflects the intent of lawmakers to regulate data-collection and -sharing practices, and illustrates how important it is for U.S. organizations to comply with emerging global standards (i.e., GDPR) — and that includes financial institutions.

Financial institutions are more likely to have prepared for GDPR than organizations in other sectors. For example, prior to GDPR enactment, more than 27 percent of financial services firms were already prepared to comply with GDPR requirements that call for security breaches be reported to authorities within 72 hours of breach awareness (vs. just 20 percent in other industries).[3]

This new readiness is important — because there have been a high number of banking, credit, and financial institutions that have experienced data breaches recently as compared to other industries. The overall number of U.S. data breach incidents in 2017 was a record 1,579, with 8.5 percent in the banking/credit/financial sector.[4] Some of the largest breaches in history have involved financial services companies, including Equifax Inc. in 2018 (143 million U.S. accounts and 400,000 UK accounts) and Heartland Payment Systems in 2008 (information on 130 million customers).[5]

With or without the requirements being imposed by GDPR, one thing is certain: breaches may be more costly in the future for institutions that hold information of EU data subjects, given that penalties for violating GDPR data security regulations are severe. Fines for GDPR non-compliance can reach €20 million or up to 4 percent of an organization's annual worldwide revenue of the preceding financial year, whichever is greater.[6]

While compliance *risks* grab much of the attention around GDPR and other regulatory changes, *opportunities* for financial institutions abound as well. Many of the new processes and new technologies that may help institutions with data security and GDPR compliance efforts can also help to improve document workflows in ways that can improve customer satisfaction, boost productivity and quality, and reduce costs.

With or without the requirements being imposed by GDPR, one thing is certain: breaches are likely to be more costly in the future, given that penalties for violating GDPR data security regulations are severe.

[3] Joe Bernik, "Financial Services and GDPR: What 200 Professionals Told Us about Their Data Protection," McAfee, April 12, 2018.

[4] "2017 Data Breach Year-End Review," Identity Theft Resource Center® and CyberScout®.

[5] Ellen Zhang, "The Top 10 FinServ Data Breaches," Digital Guardian, Sept. 12, 2018.

[6] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

GDPR Basics[7]

The GDPR replaced Data Protection Directive 95/46/EC, and is intended to harmonize data privacy laws across EU member states. It assigns control of personal data to individuals in the EU and incorporates an array of new rights for EU data subjects, including the right to:

Access information about personal data: An EU data subject has the right to obtain from data controllers confirmation as to whether or not personal data concerning him or her is being processed, and, where that is the case, access to such personal data. Such EU data subjects can also have the right to obtain information on, among other things, the purpose of the processing, the categories of personal data, the recipients or categories of recipient to whom personal data has been disclosed, etc.

Be forgotten: An EU data subject has the right to obtain from controllers the erasure of personal data concerning him or her, without undue delay, and controllers are obligated to erase personal data without undue delay, if certain circumstances apply.

Automated individual decision-making, including profiling: An EU data subject has the right to not be subject to a decision based solely on automated processing, including profiling. The law regulates, among other things, the profiling of a person for the purpose of analyzing or predicting the individual's personal preferences, behaviors, and attitudes.

Consent: Unless expressly allowed by law, an EU data subject's personal data cannot be processed without his or her consent. Consent must be freely given, specific, informed, via an unambiguous indication of the EU data subject's agreement to the processing of personal data (e.g., by a written statement, ticking a box when visiting an internet website). Pre-ticked boxes or inactivity do not constitute consent.

Data portability: An EU data subject has the right to receive personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, machine-readable format, and has the right to transmit the data to another controller, if certain circumstances apply.

[7] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Time limits: Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes.

GDPR is likely to alter the ways organizations collect and manage personal information. It defines and may require "data controller" and "data processor" roles for organizations dealing with EU data subjects, and identifies required processes that may apply to both (appointment of a "data protection officer," response to a breach, etc.):

Controller is the natural or legal person, public authority, agency, or other body that alone or jointly with others determines the purposes and means of the processing of personal data. The controller implements appropriate technical and organizational measures to ensure and demonstrate that data processing is performed in accordance with GDPR, including application of data-protection policies.

Processor is the natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller. Processors need to meet the standards set forth by controllers. Where processing is done for a controller, the controller needs to ensure that the processor has sufficient guarantees to implement appropriate technical and organizational measures to comply with GDPR and can ensure the protection of the rights of EU data subjects.

Data protection officer: Controller and processor shall designate a data protection officer in any case where processing is carried out by a public authority or body, except for courts acting in their judicial capacity; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 of the GDPR and personal data relating to criminal convictions and offenses referred to in Article 10 of the GDPR.

Lastly, and of importance to U.S. financial institutions, GDPR extends to foreign organizations processing the data of individuals in the EU. For example, if a customer is located in the EU, all EU personal data that is transmitted to the U.S. institution can be subject to the GDPR. Non-EU established businesses are subject to the GDPR where they process personal data of data subjects in the EU in connection with behavior of individuals in the EU.

Catching Up to GDPR

The GDPR is a complex set of regulations; it's no wonder that more than two years after the EU approved them in April 2016, compliance challenges remain for many financial institutions, including, but not limited to:

- Addressing accountability requirements — both compliance and proof of compliance are required
- Documenting data-management protocols and processes (i.e., information workflows)
- Reviewing data-collection procedures to ensure consent
- Proving the necessity of processing personal data, if and when collected
- Securing vulnerable systems against a range of cyberthreats (malware, ransomware, etc.)
- Establishing procedures to quickly report breaches.

Even worse, some U.S. financial institutions may be unaware of the full extent of the GDPR and its impact. Given the high volume of financial trade with EU countries — in 2017, the EU imported €21.5 billion in financial services from the United States[8] — many financial institutions have large numbers of EU customers.

Exposure to GDPR does not require *physically* conducting business in the EU (the establishment of offices or branches) or even providing services into the EU; mere *holding of data* on EU individuals is also covered under GDPR. U.S. financial institutions should establish policies and infrastructures that meet GDPR thresholds for information they likely hold.

Some U.S. financial institutions may be unaware of the full extent of the GDPR and its impact.

[8] International trade in services (since 2010), Eurostat, July 11, 2018.

Minimize GDPR Risks

Financial institutions capturing and holding EU personal data should know what data is collected; why data is being collected; where data is held and processed; and who has access. Like many industries, the finance sector includes multinational organizations with data consolidated into massive enterprise systems; nonetheless, many are challenged to find GDPR answers — by legacy systems, paper-based records, and varying software applications among offices, branches, subsidiaries, partners, and affiliates. To help meet GDPR requirements, financial institutions typically should develop data-centric strategies for which all departments, functions, and technology platforms contribute to a solution (i.e., no rogue plans) with role-specific objectives and GDPR activities:

- *The enterprise:* The company should develop an overall strategy based on a review of where personal data is held (systems) and its ability to manage this information in ways that help them to be compliant with GDPR. An enterprise-wide strategy can establish GDPR awareness, requirements, and enforcement methods for various functions and departments.
- *Information technology (IT) departments:* IT departments should develop technical strategies that align with those of their companies, possibly integrating new systems and networks with legacy technologies to accommodate personal data requirements and requests; improve security; and deploy breach-awareness capabilities. IT also plays a key role in data governance and systems strategies.
- *Procurement:* The company should develop or refine guidelines and support contracts to minimize GDPR-compliance risks associated with partners and vendors for services (consulting, research, technical); goods (systems, applications, office devices); and other services (data processors, hosting firms).

The organization and all parties involved with it can take steps to minimize risks of GDPR non-compliance and streamline personal information workflows by, among other things:

Understanding why data is collected, and where it's kept

It's important for financial institutions to document *why* they collect any piece of personal information from EU data subjects, *what* they do with it, and to *whom* it is disclosed — even if the organization did not collect the information in the first place (i.e., it was provided by other organizations). Despite widespread digitization within the finance sector, many U.S. financial institutions still have legacy information-management practices that struggle to achieve common needs, let alone GDPR compliance: limited or missing authorizations for information; non-standardized information collection and handling processes; mixed file formats that make data searches inefficient or impossible, etc.

At the same time, the volume of data collected and held in the finance sector is enormous.

For example, the top three U.S. credit-card companies alone had more than 600 million card holders in 2018: Visa (323 million), MasterCard (191 million), and Chase (93 million).[9] Making matters worse, some financial institutions may have complex, siloed information workstreams with cumbersome processes and incomplete documentation.

Even where a company has consistent practices and processes for managing information at headquarters and major offices, it's possible that some locations and suppliers will not strictly adhere to those same rules. Mapping information workstreams is a good first step for financial institutions to track the collection and processing of personal information, as well as GDPR compliance requirements.

While there is no specific GDPR requirement for data mapping itself, this exercise is a key component of compliance.[10] Why? Because mapping can help to identify *where* personal information is kept (e.g., systems, contact lists, email addresses) and to optimize *how* this information is managed in ways consistent with GDPR. For example, do the location and access provisions for a specific type of data make it easy to find and revise or delete records upon request? Can the financial institution identify and remove unnecessary personal information — across all functions, departments, and offices?

Just as important, data mapping can identify delays and waste in document management processes — enhancing collaboration and productivity.

Accommodating customized data requirements

The GDPR's right of information and access to personal data grants EU data subjects the right to information about data collected about them, and gives data subjects information necessary to ensure fair and transparent processing.[11] To do this, financial institutions may consider the implementation of personal-data workflows that can improve compliance with GDPR requirements; automating these new processes can help administrators in meeting EU data subject requests.

Developing consistent, enterprise-wide, information-governance strategies

All actions involving personal data — collecting, hosting, managing and sharing records, removing data, working with support vendors, etc. — must be aligned with enterprise-wide GDPR strategies, policies, and technologies, from headquarters out to affiliates. Even if a financial institution is defined solely as a data controller for a given data set (i.e., it collected and defined how the data is to be used and processed), it should ensure that its data processor(s) are GDPR-compliant, too.

Even where a company has consistent practices and processes for managing information at headquarters and major offices, it's possible that some locations and suppliers will not strictly adhere to those same rules.

[9] "Leading credit card companies in the United States in 2018, by number of card holders (in millions)," Statista,2018.

[10] Alison Cregeen, "A practical guide to data mapping for GDPR compliance," PWC, March 6, 2018.

[11] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Ideally, financial institutions will have taken steps to become GDPR-compliant long before May 2018, for example:

1. Assembling a cross-functional working group to review and assess GDPR and its impact across the organization.
2. Conducting data mapping of personal information workstreams and assessment of GDPR-compliance gaps (e.g., potential for unauthorized access, inability to quickly remove or alter data, unauthorized collection of unnecessary personal information).
3. Establishing policies and governance around GDPR data management.
4. Trialing new practices in model areas (e.g., office, department) to test GDPR risk exposure and compliance.
5. Communicating GDPR policies and procedures throughout the organization and assembling and deploying subgroups as necessary to implement new practices.
6. Routinely reassessing GDPR risk exposure and compliance.

For example, Bank of America Merrill Lynch, a division of Bank of America, established an enterprise-wide GDPR program to ensure that employees, partners, and vendors process personal data in compliance with GDPR requirements. The program has key executive sponsorship; covers subsidiaries and affiliates; and involves a review of data-processing activities (e.g., applications, databases, policies, processes). "Bank of America Merrill Lynch leverages a network of country compliance officers and a global Privacy Legal and Compliance team to ensure sustainable compliance with the GDPR going forward."[12]

[12] GDPR, Bank of America Merril Lynch.

Leverage Opportunities in GDPR Compliance Efforts

Some improvement-minded financial institutions are changing their data processes, workflows, and document-management systems to improve data security — but with other gains in mind, too. Indeed, for some, GDPR compliance is a vehicle to leverage data workflow improvements to enhance day-to-day operations and bring greater value to customers, staff, and stakeholders. This may be done by implementing new best practices, new work models, and new technologies that impact:

- *Data workflows:* Lean financial institutions — those seeking to continuously remove waste and costs and add value for customers — have used process mapping for decades to identify bottlenecks and wastes that can drain profits even as they frustrate customers, executives, managers, and frontline staff. Mapping may not only define new document workflows that can help to address GDPR requirements but can also help to streamline *all* document workflows. For example, moving from mixed-media information formats to all-digital data workflows can improve the overall efficiency of office operations, which can deliver financial benefits.

  Mapping also identifies gaps in security and information controls, which can help to remediate potential security liabilities and establish a log of activities through which personal information travels, from handling to authorized access.

- *Data security:* Financial institutions can implement new personal data workflows with security controls and automated tracking mechanisms to help document GDPR-compliant collection and management. Data protection technologies can be integrated into processes to help to minimize the risk of security breaches, such as incorporating protected and/or sensitive content into a regulated workflow as soon as data is received; limiting unauthorized access to office devices; and ensuring that digital communications leverage classification tools to accurately catalog, store, and protect information.

Some improvement-minded financial institutions are changing their data processes, workflows, and document-management systems to improve data security — but with other gains in mind, too.

- *Data-breach response:* GDPR may drive many financial institutions to limit data access (including printers, copiers, scanners, smart phones, and other touchpoints) in order to limit breaches. And because GDPR requires that a breach be reported to authorities within 72 hours of discovery — along with identifying both the cause and likely consequences[13] — automated GDPR-alert capabilities and proactive procedures can help. New technologies that alert administrators automatically of words used or actions taken that may indicate a breach can help to compile an investigative trail, by capturing log-in information, data, and images from office devices, etc. These plans and technologies also can help financial institutions in contacting other authorities, business partners, and individuals regarding security breaches that may not involve GDPR and EU data subjects.
- *Deploy and model new best practices and technologies:* Financial institutions can embrace the GDPR as a means to prepare themselves for a new era of personal-information management. Protecting personal information privacy by establishing new infrastructure and policies can not only improve data security but also can enhance efficiency across the enterprise. This provides a template to share with those supporting the company for managing personal information within their organizations — involving EU data subjects and others — and also can be applied to new locations and acquisitions as a company expands.

U.S. financial institutions find themselves on the frontline of protecting personal information; GDPR raises the stakes even higher. Is your financial institution ready for a brave new world of data risk — and opportunity?

Protecting personal information privacy by establishing new infrastructure and policies will not only improve data security but also enhance efficiency across the enterprise.

[13] Regulations, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union.

Canon U.S.A. is not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the suggestions discussed in this white paper. Canon USA does not make any warranties concerning the accuracy or completeness of the opinions, data and other information contained in this content and, as such, assumes no liability for any errors, omissions or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data or other information.

Canon U.S.A. does not provide legal counsel or regulatory compliance consultancy, including without limitation, GDPR, Sarbanes-Oxley, HIPAA, GLBA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.

Prepared as of 2.8.19. Rules and regulations may change from time to time. As stated above, please have your own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance.