The MPI Group
People. Purpose. Profits.

U.S. Law Firms 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 enactment of the General Data Protection Regulation (GDPR) in the European Union is challenging law firms around the world regarding client information security as never before. Yet amid general concern and uncertainty in the sector about GDPR compliance, some firms see opportunity.

Why?

Because leaders at these organizations understand that streamlined information workflows can not only help with security and GDPR compliance efforts, but also deliver a competitive edge by making their organizations more responsive and agile. Even more compelling is the opportunity to model and implement these new processes for their clients, which may be even *less* likely to be prepared for GDPR.

New Standards and New Risks

Law firms have long accepted immense responsibility for holding and securing client information. Attorney-client privilege, which began as early as 1654 in England,[1] is now one of the oldest rules in U.S. law for protecting an individual's information. Yet four centuries ago, no one could have imagined the technical issues law firms face in protecting client information from unauthorized access. Nor could anyone have envisioned the increasing array of penalties that governments can impose on businesses and on law firms — in response to consumer demand for privacy protections — should they fail to do so.

After decades in the making and a two-year period for companies to prepare, on May 25, 2018 the European Union began enforcement of the GDPR. The rule covers the "protection of natural persons with regard to the processing of personal data and on the free movement of such data,"[2] and 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 model. For example, in June 2018, California passed a digital privacy law, effective January 1, 2020, that gives consumers more control over the personal information that covered businesses collect from them.[3] And as inappropriate uses of personal data by businesses and hackers continue to make news, increasingly stringent regulations may arise.

The California Consumer Privacy Act reflects the intent of lawmakers around the world to regulate data-collection and -sharing practices among businesses, and illustrates how important it is for

Four centuries ago, no one could have imagined the technical issues law firms face in protecting client information from unauthorized access.

[1] Geoffrey C. Hazard Jr., "An Historical Perspective on the Attorney-Client Privilege," *California Law Review,* September 1978.

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

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

U.S. businesses to comply with emerging global standards (i.e., GDPR).

"Businesses," of course, includes law firms. Unfortunately, many law firms lag in adoption of effective data security practices — and often fall victim to unauthorized data use. Some 22 percent of law firms have experienced a security breach at some point (e.g., lost/stolen computer or smartphone, hacker, break-in, or website exploit), up from 14 percent in 2016. Firms with 10 to 49 attorneys reported the highest percentage of security breaches, at 35 percent.[4] In just one example of ongoing risks, the FBI issued a Private Industry Notification in 2016 to law firms — warning that hackers were targeting international law firms as part of an insider trading scheme.[5]

GDPR will make many of these breaches even costlier in the future, given that penalties for violating its data security regulations are severe. Fines for GDPR non-compliance can reach up to €20 million or 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 law firms abound as well. Why? Because many of the new processes and new technologies required for data security and GDPR compliance can also help to improve document workflows in ways that may boost efficiency and reduce costs.

[4] David Ries, *ABA Techreport 2017: Security,* American Bar Association.

[5] Gabe Friedman, "FBI Alert Warns of Criminals Seeking Access to Law Firm Networks," *Big Law Business,* March 11, 2016

[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.

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

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.

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.he future and can strengthen relationships with suppliers and customers.

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.

Lastly, and of importance to U.S. law firms, GDPR extends to foreign organizations processing the data of EU subjects. For example, if a law firm's corporate client is located in the EU, the EU personal data handled by the U.S. firm 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 the offering of goods or services or monitoring the behavior of individuals in the EU.

Catching Up to GDPR

The GDPR is a complex set of regulations; it's no wonder that even two years after the EU approved them in April 2016, compliance challenges remain for many organizations, including:

- 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, many U.S. companies and law firms may be unaware of the full extent of the GDPR, and its impact on their businesses. Exposure to GDPR does not require *physically* conducting business in the EU or selling goods or services into the EU; mere *holding of data* on EU individuals is also covered under GDPR. Firms *considering* doing business in the EU may want to consider establishing policies and infrastructures that can meet the GDPR threshold.

Business relationships may also be at risk for U.S. law firms. Many U.S. companies conducting business in the EU expect their U.S. law firms to offer counsel on how to comply with GDPR and minimize their exposures. In 2017, U.S. exports of goods and services to Europe were $632.7 billion, up 4.9 percent from 2016, and imports from Europe were $741.6 billion, up 5.8 percent from 2016 *(Figure 1)*.[8] Law firms that are sufficiently versed in GDPR may be able to provide qualified counsel to their clients.

Figure 1. 2017 U.S. International Trade with Europe

Rank	Exports	$ billions
1	Capital goods except automotive	$127.4
2	Other business services	$84.4
3	Industrial supplies and materials	$82.7
4	Consumer goods except food and automotive	$67.9
5	Charges for the use of intellectual property	$64.7
	Other goods and services	$205.6

Rank	Imports	$ billions
1	Consumer goods except food and automotive	$143.8
2	Capital goods except automotive	$136.2
3	Industrial supplies and materials	$98.9
4	Automotive vehicles, parts, and engines	$64.5
5	Other business services	$52.2
	Other goods and services	$246.0

[8] "Europe — International Trade and Investment Country Facts," Bureau of Economic Analysis, U.S. Department of Commerce

Minimize GDPR Risks

Corporate clients doing business in the EU might assume that their legal representatives have taken appropriate measures to comply with GDPR, ensuring that information about EU data subjects passed from client to law firm are handled via appropriate policies and procedures. Law firms managing EU personal data should review their document and information management procedures specific to their roles as "data controllers" (e.g., holding and using data on EU employees and EU clients) and/or "data processors" (e.g., receiving, managing, and using EU personal data for controllers). In these roles they may be able to minimize risks of GDPR non-compliance and enhance information security by:

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

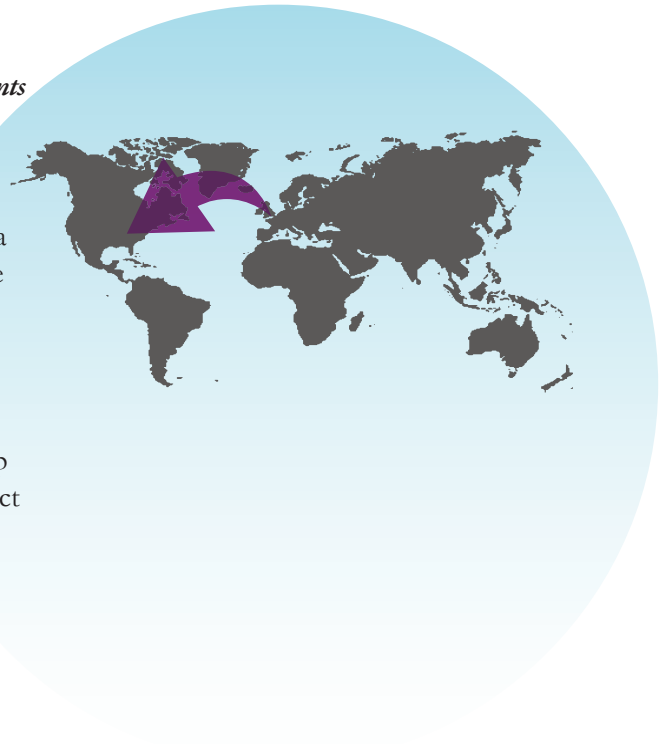
All businesses should document *why* they collect any piece of personal information from EU data subjects, *what* they do with it, and to *whom* it is disclosed — even if the organization did not collect the information in the first place (i.e., it was provided by other organizations). Many U.S. companies may have legacy information-management practices that struggle to achieve business 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.

Large firms may have complex information workstreams with less than ideal processes and incomplete documentation. Mapping information workstreams is a good first step for firms of any size to track the collection and processing of personal information, as well as adherence to GDPR compliance requirements. (Collection and processing requirements for smaller organizations — fewer than 250 employees — are not as stringent as those for larger firms, but still exist.)

While there is no specific GDPR requirement for data mapping itself, data mapping can be regarded as a key component of compliance.[9] Why? Because mapping can help to identify *where* personal information is kept (e.g., systems, contact lists, email addresses) and help to optimize *how* this information is managed in ways consistent with GDPR efforts. 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 firm identify and remove unnecessary personal information?

Just as important, data mapping can identify delays and waste in document management processes — setting the stage for improvements that may boost both security and efficiency.

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



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.[10] To do this, law firms may consider the implementation of personal-data workflows that comply with GDPR requirements; automating these new processes can help administrators in meeting EU data subject requests.

Developing consistent, firm-wide, information-governance strategies

All actions involving personal data — collecting, hosting, managing client contacts, removing data, working with support vendors, etc. — can be aligned with firm-wide GDPR strategies and technologies. For example, even if the law firm is defined solely as a data controller for a given data set (i.e., the firm collected and defined how the data is to be used and processed), it should ensure that its data processor(s) are GDPR compliant, too.

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

Leverage Opportunities in GDPR Compliance

Many improvement-minded firms are changing their data processes, workflows, and document-management systems to help improve data security — but with other gains in mind, too. Indeed, for some U.S. law firms, GDPR compliance is a vehicle to leverage data workflow improvements to enhance day-to-day operations and bring greater value to clients. This can be done by implementing best practices, new work models (e.g., use of third-party, on-demand lawyers), and new technologies that impact:

- *Data workflows:* Lean organizations — those seeking to continuously remove waste and costs and add value for customers and clients — have used process mapping for decades to identify bottlenecks that delay service to customers, and wastes that drain profits and frustrate staff, employees, business partners, and customers/clients. Mapping can not only define new document workflows that can help with some GDPR requirements, but can also help to streamline document workflows. For example, moving from paper or mixed-media information formats to all-digital data workflows can improve the overall efficiency of office operations.

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

- *Data security:* Firms should consider new, more secure personal data workflows and the use of automated tracking mechanisms that may help to document GDPR-compliant collection and management. Data protection technologies can be integrated into business processes to help 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 help accurately catalog, store, and protect information.

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

- *Data-breach response:* GDPR may drive many organizations 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,[11] automated GDPR-alert capabilities and proactive procedures can help. Technologies that alert administrators automatically of breaches may help to compile an investigative trail, capturing log-in information, data, and images from office devices, etc. These plans and technologies may also help law firms in contacting other authorities, business partners, and customers regarding security breaches that do not involve GDPR and EU data subjects.
- *Deploy and model new best practices and technologies:* Law firms can embrace the GDPR as a means to prepare themselves — and their clients — for a new era of personal-information management. Protecting client privacy by establishing new infrastructure and policies may not only improve data security but may also enhance efficiency across the firm. This can provide a template to share with clients and potential clients of how to manage the personal information within their organizations — involving EU data subjects, California citizens, and others.

Attorneys have always prospered by being trusted advocates for their clients; GDPR compliance requires bringing those same attributes into the digital age.

Is your firm ready for a brave new world of risk — and opportunity?

Attorneys have always prospered by being trusted advocates for their clients; GDPR compliance requires bringing those same attributes into the digital age.

[11] 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.